ExtremeCloud IQ Controller Deployment Guide

Version 10.07.01

9037936-00 Rev. AA
October 2023

Copyright © 2023 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Table of Contents

Preface vii
Conventions vii
Text Conventions vii
Documentation and Training ix
Open Source Declarations ix
Training ix
Send Feedback ix
Help and Support x
Subscribe to Product Announcements x
AP Regulatory Information xi

Deploy ExtremeCloud IQ Controller 12
VE6120K, VE6125K Virtual Appliances 12
VE6120H Virtual Appliance 13
VE6120 Virtual Appliance 13
VE6125 Virtual Appliance 14
Supported Appliance Specifications 14
Discovery and Registration 17
Discovery Process for APs and Adapters in a Centralized Site 18
Switch Discovery Process 20
Sites 22
Device Groups 23

Configuring DHCP, NPS, and DNS Services 25
DHCP Service Configuration 25
Configuring DHCP on Windows Server 2012 R2 25
Configuring DHCP on a Red Hat Linux Server 41
Configuring the ExtremeCloud IQ Controller as an NPS Client 44
NPS Service Configuration 45
Add a New Network Policy 45
DNS Service Configuration 50
Configuring DNS for Wireless AP Discovery 51
Configuring DNS on a Linux Server 52
Configure ExtremeCloud IQ Controller for Local DHCP Management 53
Add a Physical Interface 54
Local DHCP Settings 55

Centralized Site with an Internal Captive Portal 57
Deployment Strategy 57
Adding a Centralized Site with Device Group 57
Configuring an Internal Captive Portal 59
Specifying B@AC Network Topology 60
Configuring a Captive Portal Network 61

Working with Internal Captive Portal Engine Rules....62
Editing Device Group Profile for Network and Role....63
Creating Adoption Rules....65

Centralized Site with a AAA Network....68
Deployment Strategy....68
Configuring a AAA Network....68
Creating an Engine Rule....69
Creating a Policy Role....70
Applying a AAA Network and Role to the Device Group....71

Mesh Point Network Configuration....73
Deployment Strategy....73
Mesh Point Network Settings....74
Configure Device Groups for Mesh Point....74
Advanced Configuration Profile and Mesh Device Settings....76
Profile Advanced Settings....76
Edit Mesh Device Settings....77
Configure Transparent Bridge....80

Configuring an External NAC Server for MBA and AAA Authentication.... 82
Deployment Strategy....82
Configuring the External NAC Server....83
Network with Default Auth Role....85
Configuring an MBA Network....85
Configuring a AAA Network....86
Network with Pass-Through External RADIUS....88
Configuring an MBA Network....88
Configuring a AAA Network....89

Manage RADIUS Servers for User Authentication.... 92
RADIUS Settings....93
Advanced RADIUS Settings....93
Configure a Pass Through Rule....95

External Captive Portal on a Third-Party Server....96
Firewall Friendly External Captive Portal Flow of Events....97
FF-ECP on ExtremeCloud IQ Controller....97
Configure the Firewall....99
Configure an External Captive Portal....99
Understand Processing Performed by the ECP....100
The Redirection URL Sent from ExtremeCloud IQ Controller....100
Compose the Login or Splash Screen Page....111
Approve the Client....111
Compose the Redirection Response Sending the Browser back to the Appliance....112
Signing the Redirection to ExtremeCloud IQ Controller....112
Case 1: When a RADIUS Server Authenticates the Client....113
Case 2: When the ECP is the Final Authority....115

Access Control Rules for Admin Portal Access.... 119
Deployment Strategy....119
Configure Access Control Group....120
Default Access Control Groups....121

Configure Admin Access Policy Role....122
Configure Access Control Rule....123
Default Access Control Rules....125
Define Rule Precedence....126

Centralized Web Authorization....127
Deployment Strategy....127
CWA with ISE Deployment....128
AAA Policy Network Configuration — ISE....128
CWA Network Settings — ISE....136
CWA Policy Redirection Role — ISE....139
CWA Server Configuration — ISE....141
CWA with ExtremeControl Deployment....145
Configure AAA Policy — ExtremeControl....145
CWA Network Settings - ExtremeControl....149
CWA Policy Redirection Role — ExtremeControl....152
CWA Server Configuration — ExtremeControl....154

NAI Routing and Dynamic Discovery....158
AAA Policy Settings for NAI Routing....158
Configure a Regular Expression Realm....161

Deploying ExtremeCloud IQ-SE as an External Captive Portal....163
Deployment Strategy....163
Configuring an External Captive Portal Network....164
Editing the Configuration Profile for Network and Roles....168
ExtremeCloud IQ Controller Default Pass-Through Rule....168
Adding ExtremeCloud IQ Controller as a Switch to ExtremeCloud IQ - Site Engine....170
Editing the Unregistered Policy on ExtremeCloud IQ - Site Engine....175
Editing the ExtremeCloud IQ - Site Engine Profile for Policy and Location-Based Services....177

Deploying an ExtremeGuest External Captive Portal....185
Deployment Strategy....185
Configure an ExtremeGuest Server....186
Configure an ExtremeGuest Captive Portal Network....186
Configuration Settings on ExtremeGuest....187

Deploying Client Bridge....189
Deployment Strategy....189
AP Client Bridge....189
Configure Client Bridge....191

Deploying an Availability Pair....196

Deploying an Availability Pair with Extreme AirDefense....199
Deployment Strategy....199
Deployment Procedure....199
Configuring the Centralized Site with an AP3915 Profile....200
Configuring AirDefense....200

Deploying an Availability Pair and External Captive Portal....202
Deployment Strategy....202
Deployment Procedure....202

Configuring External Captive Portal Network....203
Editing the Device Group Profile for ECP Network....206

Integration with ExtremeCloud IQ....207
Deploy Universal APs....207
Onboarding Universal APs — ExtremeCloud IQ....208
Onboard a Controller to ExtremeCloud IQ....213
Adding a Controller — Welcome Dialog....214
Add a Controller — Quick Add....216
Access the Controller UI from ExtremeCloud IQ....218

PHP External Captive Portal, Controller's Firewall Friendly API....219
net-auth.php....219
login.php....223
common_utilities.php....225
crypt_aws_s4.php....229
ffecp-config.php....234

Index....236

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Conventions

To help you better understand the information presented in this guide, the following topics describe the formatting conventions used for notes, text, and other elements.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions

Table 1: Notes and warnings (continued)

Icon	Notice type	Alerts you to...
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{` **`x`** `|` **`y`** `|` **`z`** `}`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x` `|` **`y`**	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.

Table 3: Command syntax (continued)

Convention	Description
...	Repeat the previous element, for example, *member*[*member*...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

AP Regulatory Information

For regulatory information for the ExtremeCloud IQ Controller supported access point models and appliances, refer to the appropriate *Installation Guide*.

Deploy ExtremeCloud IQ Controller

VE6120K, VE6125K Virtual Appliances on page 12
VE6120H Virtual Appliance on page 13
VE6120 Virtual Appliance on page 13
VE6125 Virtual Appliance on page 14
Supported Appliance Specifications on page 14
Discovery and Registration on page 17
Sites on page 22
Device Groups on page 23

The Deployment Guide will guide you through the process of deploying your access points using ExtremeCloud IQ Controller. The instructions will provide a flow of tasks from creating a site, through captive portal and network configuration, to developing adoption rules that will automatically organize your APs into proper device groups upon registration with ExtremeCloud IQ Controller.

The purpose of the Deployment Guide is to get you up and running quickly, taking you through the full deployment process. If there are concepts or parameter options you do not understand, consult the User Guide or ExtremeCloud IQ Controller Online Help system for detailed information.

VE6120K, VE6125K Virtual Appliances

VE6120K for KVM offers elasticity with support for small, medium, and large deployments. VE6125K targets extra large KVM deployments of up to 4000 access points. The larger capacity offers support for customers who manage a large deployment from a virtual installation. The VE6125K X-Large configuration provides capacity parity with the E2120:

- Uses the same licensing procedure as the VE6120
- Is entitled per the 30324/30326 activation keys
- Accepts the same capacity keys as other models

Note
VE6120K and VE6125K use separate image files. You cannot upgrade from one VM model to another.

Virtual Machine Upgrade File Formats:

- VE6120K — .dve
- VE6125K — .mfe

Requirements for the ExtremeCloud IQ Controller VE6120K and VE6125K models are listed in Supported Appliance Specifications on page 14.

Related Topics

Supported Appliance Specifications on page 14

VE6120H Virtual Appliance

VE6120H for Microsoft Hyper-V offers elasticity with support for small, medium, and large deployments:

- Uses the same licensing procedure as the VE6120.
- Is entitled per the 30324/30326 activation keys.
- Accepts the same capacity keys as other models.
- Supported on Windows Server 16 (minimal support). The lowest supported VMBUS is version 3.0.

Virtual Machine Upgrade File Format:

- VE6120H — .spe

Requirements for the ExtremeCloud IQ Controller VE6120H model are listed in Supported Appliance Specifications on page 14.

For installation information, see *VE6120H Virtual Appliance Installation Guide Microsoft Hyper-V Platform* located in the Extreme Networks documentation portal.

Related Topics

Supported Appliance Specifications on page 14

VE6120 Virtual Appliance

The VE6120 Appliance is a virtual machine providing management of up to 1,000 APs. It offers support for small, medium, and large deployments and requires activation and device adoption keys.

Virtual Machine Upgrade File Formats:

Note

VE6120, and VE6125 use separate .ova files. You cannot upgrade from one VM model to another.

Virtual Machine Upgrade File Formats:

- VE6120 — .dle
- VE6125 — .rse

Requirements for the ExtremeCloud IQ Controller VE6120 model are listed in Supported Appliance Specifications on page 14.

For installation information, see *VE6120/VE6125 Virtual Appliances Installation Guide VMware® Platform* located in the Extreme Networks documentation portal.

Related Topics

Supported Appliance Specifications on page 14
VE6125 Virtual Appliance on page 14

VE6125 Virtual Appliance

VE6125 targets extra large deployments of up to 4000 access points. The larger capacity offers support for customers wanting to manage a large deployment from a virtual installation. The VE6125 X-Large configuration provides capacity parity with the E2120. Customers with large installations of up to 4000 APs have the option to manage their infrastructure via a pair of hardware appliances, the E2120 or in virtual configuration options, the VE6125:

- Requires a VMWare Enterprise license.
- Uses the same licensing procedure as the VE6120.
- Is entitled per the 30324/30326 activation keys.
- Accepts the same capacity keys as the hardware model E2120.

Note
VE6120, and VE6125 use separate .ova files. You cannot upgrade from one VM model to another.

Virtual Machine Upgrade File Formats:

- VE6120 — .dle
- VE6125 — .rse

Requirements for the ExtremeCloud IQ Controller VE6125 model are listed in Supported Appliance Specifications on page 14.

For installation information, see *VE6120/VE6125 Virtual Appliances Installation Guide VMware® Platform* located in the Extreme Networks documentation portal.

Related Topics

Supported Appliance Specifications on page 14
VE6120 Virtual Appliance on page 13

Supported Appliance Specifications

ExtremeCloud IQ Controller supports the following virtual appliances:

- VMWare:
  - VE6120
  - VE6125
- KVM
  - VE6120K
  - VE6125K
- Microsoft Hyper-V
  - VE6120H

And the following hardware appliances:

- E1120
- E2120
- E2122
- E3120
- E3125

Requirements for each ExtremeCloud IQ Controller model are listed below.

Table 4: Virtual ExtremeCloud IQ Controller (VE6120 and VE6125)

Extreme Application	VE6120			VE6125
	Small	**Medium**	**Large**	**X-Large**
Total APs managed in Standalone mode	50	250	500	2000
Additional APs supported in high-availability mode	50	250	500	2000
Total managed APs per Appliance Pair	100	500	1000	4000
Total Switches managed per Appliance	50/100	100/200	200/400	200/400
Total simultaneous users in Standalone mode	1,000	4,000	8,000	16000
Additional simultaneous users in high-availability mode	1,000	4,000	8,000	16000
Total Simultaneous Users per Appliance Pair	2,000	8,000	16,000	32000
Hardware Requirements				
CPU	4 (4 distinct physical cores or 2 cores with hyper-threading)	6	8	32 (physical or hyper-threading cores)
RAM (GB)	8	16	24	32
Hard Disk (GB)	80	80	80	512

- Consult VMWare ESXi for minimum host performance requirements for virtual environment. Performance depends on network interface characteristics of underlying host and on utilization on shared interfaces by other virtual appliances.
- Follow VMWare minimum installation requirements. 10 Gbps host recommended for best results. VE6120 supports VMware ESXi 5.1 or higher. VE6125 supports VMware ESXi 5.5 or higher.

- A VMware Enterprise license is required for the VE6125.

Table 5: Virtual ExtremeCloud IQ Controller VE6120H

Extreme Application	VE6120H		
	Small	**Medium**	**Large**
Total APs managed in Standalone mode	50	250	500
Additional APs supported in high-availability mode	50	250	500
Total managed APs per Appliance Pair	100	500	1000
Total Switches managed per Appliance	50/100	100/200	200/400
Total simultaneous users in Standalone mode	1,000	4,000	8,000
Additional simultaneous users in high-availability mode	1,000	4,000	8,000
Total Simultaneous Users per Appliance Pair	2,000	8,000	16,000
Hardware Requirements			
CPU	4 (4 distinct physical cores or 2 cores with hyper-threading)	6	8
RAM (GB)	8	16	24
Hard Disk (GB)	80	80	80

Table 6: Virtual ExtremeCloud IQ Controller (VE6120K and VE6125K)

Extreme Application	VE6120K			VE6125K
	Small	**Medium**	**Large**	**XLarge**
Total APs managed in Standalone mode	50	250	500	2000
Additional APs supported in high-availability mode	50	250	500	2000
Total managed APs per Appliance Pair	100	500	1000	4000
Total Switches managed per Appliance	50/100	100/200	200/400	200/400
Total simultaneous users in Standalone mode	1,000	4,000	8,000	16000
Additional simultaneous users in high-availability mode	1,000	4,000	8,000	16000
Total Simultaneous Users per Appliance Pair	2,000	8,000	16,000	32000

Table 6: Virtual ExtremeCloud IQ Controller (VE6120K and VE6125K) (continued)

Extreme Application	VE6120K			VE6125K
Hardware Requirements				
CPU	4	6	8	20 Cores
RAM (GB)	8	16	24	32
Hard Disk (GB)	80	80	80	250

Table 7: ExtremeCloud IQ Controller Hardware

Supported Features	E1120	E2120/ E2122	E3120	E3125
Total APs managed per appliance pair	250	4,000	20,000	20,000
Total APs managed in stand-alone mode per appliance	125	2,000	10,000	10,000
Additional APs supported in high-availability mode	125	2,000	10,000	10,000
Total switches managed per appliance	50/100	400/800	1,000/2,000	1,000/2,000
Total simultaneous users per appliance pair	4,000	32,000	Scales up to 100,000	Scales up to 100,000
Total simultaneous users in stand-alone mode per appliance pair	2,000	16,000	Scales up to 50,000	Scales up to 50,000
Additional simultaneous users in high-availability mode	2,000	16,000	Scales up to 50,000	Scales up to 50,000
Dual, hot swappable power supplies	Not applicable	Sold Separately	Sold Separately	Sold Separately
Maximum throughput (Mbps), Mixed (RFC2544)/Encrypted	3730 /2140	18500 / 18000	54,000 / 25,500	72,000 / 31,500".

Related Topics

VE6120K, VE6125K Virtual Appliances on page 12
VE6120H Virtual Appliance on page 13
VE6125 Virtual Appliance on page 14

Discovery and Registration

Wireless devices (APs and SA201 adapters) discover the IP address of ExtremeCloud IQ Controller using a sequence of mechanisms that allow for the possible services available on the enterprise network. The discovery process is successful when the AP/adapter successfully locates a controller to which it can register. Ensure that the

appropriate services on your enterprise network are prepared to support the discovery process.

Note
The following subnets are reserved for internal communications and Docker operations:

- 172.17.0.0/24
- 172.31.0.16/28

The ExtremeCloud IQ Controller user interface logic prevents adding addresses in these address ranges for VLAN interface references.

An access point can learn a hostname from a DHCP server. The AP reports either the discovered hostname, or an internally generated hostname (which is the AP serial number) to the controller as part of the discovery process.

- If ExtremeCloud IQ Controller does not have a current record of the AP, the controller applies the reported hostname for use in the Name and Hostname fields for the AP.
- If ExtremeCloud IQ Controller already has a record for the AP, then the controller ignores the reported hostname.
- If the AP does not report a hostname to the controller as part of the discovery process, and there is no record of the AP on ExtremeCloud IQ Controller, then the name and hostname are generated.

Enhanced Discovery can be used to onboard a Universal Access Point to ExtremeCloud IQ for local management. For more information, see Enhanced Discovery on page 211.

Note
Enhanced Discovery is supported on AP3000. It requires ExtremeCloud IQ version 23.6.1 or greater.

Discovery Process for APs and Adapters in a Centralized Site

Note
The following process outlines device discovery and registration for access points, and SA201 adapters, in a Centralized site.

ExtremeCloud IQ Controller supports Extreme Defender Adapter SA201 for the Defender for IoT solution. For more information on Extreme Defender for IoT, refer to documentation located in the Extreme Networks documentation portal.

When a wireless device is powered on, it automatically begins a discovery process to determine its own IP address and the IP address of the ExtremeCloud IQ Controller. When the discovery process is successful, the AP/adapter registers with the ExtremeCloud IQ Controller.

Enhanced Discovery

To support deployments that do not have a local network configuration for discovery, we offer an enhanced AP onboarding experience that provides indication of the specific IP address or Fully-Qualified Domain Name (FQDN) of the controllers to which the AP connects.

With Enhanced Discovery, the user assigns a selection of APs to be managed by a specific controller (or high availability pair) as part of the conversion to local operating system. Once the AP boots into the local WiNG operating system, if the discovery override is defined, the AP automatically connects to the indicated controller, bypassing the traditional discovery methods.

After registering with ExtremeCloud IQ for onboarding, the AP assumes the local WiNG operating system. After booting into the local AP image, the AP interacts with the redirector to determine if the controller list is configured. If the controller IP addresses are present, the AP attempts to connect to the defined controllers.

Note
Enhanced Discovery is supported on AP3000. It requires ExtremeCloud IQ version 23.6.1 or greater.

Related Topics

Enhanced Discovery on page 211

Discovering Centralized Site APs and Adapters

Once an AP has successfully registered with a controller, it recalls that controller's IP address, and uses that address on subsequent reboots. The AP bypasses discovery and goes straight to registration. Use the IP address of the controller to which the AP last connected successfully.

If a known controller cannot be located, take the following steps:

1. Use DHCP Option 60 to query the DHCP server for available controllers. The DHCP server responds to the AP with Option 43, which lists the available controllers.

   AP queries known ExtremeCloud IQ redirector to retrieve configured controller IP addresses or FQDNs.

   For the DHCP server to respond to an Option 60 request from an AP, configure the DHCP server with the vendor class identifier (VCI) for each AP model. Also, configure the DHCP server with the IP addresses of the controllers.
2. Use a Domain Name Server (DNS) lookup for the host name Controller.domain-name.

   The AP tries the DNS server if it is configured in parallel with SLP unicast and SLP multicast.

   If you use this method for discovery, place an A record in the DNS server for Controller.*<domain-name>*. The *<domain-name>* is optional, but if used, ensure it is listed with the DHCP server.

3. Use a multicast SLP request to find SLP SAs.

   The AP sends a multicast SLP request, looking for any SLP Service Agents providing the Extreme Networks service.

   The AP tries SLP multicast in parallel with other discovery methods.
4. Use DHCP Option 78 to locate a Service Location Protocol (SLP) Directory Agent (DA), followed by a unicast SLP request to the Directory Agent.

   To use the DHCP and unicast SLP discovery method, ensure that the DHCP server on your network supports Option 78 (DHCP for SLP RFC2610). The APs use this method to discover the controller.

   This solution takes advantage of two services that are present on most networks:

   - **DHCP** — The standard is a means of providing IP addresses dynamically to devices on a network.
   - **SLP** — A means of allowing client applications to discover network services without knowing their location beforehand. Devices advertise their services using a Service Agent (SA). In larger installations, a Directory Agent (DA) collects information from SAs and creates a central repository (SLP RFC2608).

     The controller contains an SLP SA that, when started, queries the DHCP server for Option 78 and if found, registers itself with the DA as service type Extreme Networks. The controller contains a DA (SLPD).

     The AP queries DHCP servers for Option 78 to locate any DAs. The SLP User Agent for the AP then queries the DAs for a list of Extreme Networks SAs.

     Option 78 must be set for the subnets connected to the ports of the controller and the subnets connected to the APs. These subnets must contain an identical list of DA IP addresses.

Switch Discovery Process

ExtremeCloud IQ Controller provides support for Management and Statistical services for ExtremeXOS and 200 Series switches. These switches are provisioned with built-in Zero Touch Provisioning (ZTP). ZTP provisioned switches can discover and connect to any of the following Extreme Networks Management Appliances:

- On-premises ExtremeCloud IQ Controller
- On-premises ExtremeCloud IQ - Site Engine
- ExtremeCloud™ IQ

Note
Only one appliance at a time can be configured as the Management Appliance.

When the switch is turned on, it automatically starts the Linux process `cloud-connector client`. The cloud-connector client relies on the Default VLAN 1 enabled DHCP client to discover a DHCP server. The default configuration for these switches

includes all data ports configured with VLAN 1. Any pre-configured data port can be used to connect to a DHCP Server. Simply provide an IP address and the Domain Name.

After the switch receives an IP address and a Domain Name, it begins the DNS query to find the built-in Extreme Networks Management Appliance Fully-Qualified Domain Name (FQDN):

- `extremecontrol@<domain-name>` for on-premises appliances (ExtremeCloud IQ Controller or ExtremeCloud IQ - Site Engine).

The cloud-connector tries to resolve these names in an endless round-robin loop. When any of the names are resolved to an IP address, the switch attempts connection to that IP address.

Note

Before connecting a switch to an on-premises Management Appliance:

- Within ExtremeCloud IQ Controller, configure each physical port to enable device registration:
  1. Go to **Administration** > **System**.
  2. Under **Interfaces** select **Add**.
  3. On the **Create New Interface** dialog, check **Enable Device Registration**.
- Configure a local DNS server that resolves `extremecontrol@<domain-name>` to the IP address of a ExtremeCloud IQ Controller physical port that is configured with the **Enable Device Registration** enabled.

Related Topics

Discovering Switches on page 21
Switch Discovery in an Availability Pair on page 22

Discovering Switches

A switch discovers ExtremeCloud IQ Controller by resolving the built-in Fully-Qualified Domain Name (FQDN) `extremecontrol@<domain-name>` to an IP address. `<domain-name>` is the domain assigned to the switch by the DHCP server.

To configure switch discovery, add a single `"A" record` for `extremecontrol@<domain-name>` to the local DNS server. If using a public DNS service, add the record to the DNS service. When using the public option, the DNS servers used by the switch must be integrated with the public service.

When the switch discovers ExtremeCloud IQ Controller, the device status is initially *In-Service-Trouble*. This corresponds to the cloud-connector machine state *Connecting* and is represented in ExtremeCloud IQ Controller as a yellow triangle.

Once ExtremeCloud IQ Controller acknowledges the switch configuration, the switch enters the machine state *Running*. This state is represented in ExtremeCloud IQ Controller with a green circle.

Figure 1: ExtremeCloud IQ Controller: Switch States During Discovery

Related Topics

Switch Discovery in an Availability Pair on page 22
Switch Discovery Process on page 20

Switch Discovery in an Availability Pair

When configuring ExtremeXOS switches in an ExtremeCloud IQ Controller (ExtremeCloud IQ Controller) Availability Pair, use an `"A" record` for `extremecontrol@<domain-name>`, providing an IP address for the primary ExtremeCloud IQ Controller and an IP address for the backup ExtremeCloud IQ Controller. When the first address fails, the switch attempts the second IP address. If both IP addresses fail, the switch performs a second DNS request. The switch performs the DNS request before sending an HTTPS message and does not use DNS caching.

- If both the primary and backup ExtremeCloud IQ Controller are up, all configured switches are adopted on the primary ExtremeCloud IQ Controller, and the switch sends the HTTPS message to the primary ExtremeCloud IQ Controller only.
- If the primary ExtremeCloud IQ Controller is down and the backup ExtremeCloud IQ Controller is up, the switch fails over to the backup. The switch will timeout on the primary IP address and proceed to the secondary IP address. The switch attempts to send the HTTPS message to the primary ExtremeCloud IQ Controller first because its IP address is first in the DNS reply. That attempt will timeout and the switch will send the second HTTPS to the secondary IP address. The switch continues to send HTTPS messages to both IP addresses. If the primary ExtremeCloud IQ Controller comes up, the switch sends the HTTP message to the first IP address and does not attempt the second IP address.

Related Topics

Switch Discovery Process on page 20
Discovering Switches on page 21

Sites

Use sites to define boundaries for fast roaming and session mobility without interruption. A site represents a physical, geographic area in your network. As the top-level element in the ExtremeCloud IQ Controller data model, the site runs Sessions Manager and RF Manager functions for all RF Domains in the site.

The following ExtremeWireless™ access points are supported by ExtremeCloud IQ Controller:

- AP3000/X
- AP302W
- AP305C/CX
- AP305C-1

- AP310i/e
- AP310i/e-1
- AP360i/e
- AP4000
- AP4000-1
- AP410i/e
- AP410i-1
- AP410C
- AP410C-1
- AP460i/e
- AP460C/S6C/S12C
- AP5010
- AP5050U/AP5050D
- AP505i
- AP510i/e
- AP510i-1
- AP560i/h
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

A Defender site is a Centralized site that supports SA201. It begins with the DFNDR_ prefix.

The licensing domain is defined at the site level. When configuring a site, select the Country value that matches the licensing domain of the APs that comprise the site.

Note
If the licensing domain of your AP does not match the Country assigned to the site, the AP will not display within a device group for possible selection.

Device Groups

The most simple site configuration allows for one device group for each AP/adapter model, selecting the default configuration profile and the default RF Management profile for that model.

A more complex deployment allows for more than one device group per AP model. This makes use of different profile features and/or a unique RF Management profile for each device group. With this more complex deployment, create a device group for any combination of configuration features and RF configurations.

All devices in a device group must share the following:

- AP/adapter model number
- Configuration Profile
- RF Management Profile

You have the option to discover AP/adapters before creating a device group. However, if you create the device group first, discovered devices that match the configuration profile are listed within the **Create Device Group** dialog, allowing you to simply add each AP/adapter to the device group. Furthermore, if you create a device group and an adoption rule, your newly discovered AP/adapters will be automatically added to the correct device group without your intervention.

Configuring DHCP, NPS, and DNS Services

DHCP Service Configuration on page 25
Configuring the ExtremeCloud IQ Controller as an NPS Client on page 44
NPS Service Configuration on page 45
DNS Service Configuration on page 50
Configure ExtremeCloud IQ Controller for Local DHCP Management on page 53

This chapter describes how to configure DHCP and DNS (Domain Name System) services on a Windows Server 2012 R2 or Linux server for use by ExtremeWireless Appliance and APs. In addition, the chapter explains how to configure Network Policy Server (NPS) service on Windows Server 2012 R2. Use the configuration processes in this chapter as a reference when configuring services.

Note
Windows Server 2012 R2 or Linux server may have a different configuration process than what is described here. Refer to your manufacturer's documentation for the configuration process that is specific to your server.

This section includes the following procedures:

- DHCP Service Configuration on page 25
- NPS Service Configuration on page 45
- DNS Service Configuration on page 50

DHCP Service Configuration

Before you can configure the DHCP service, you must install it on the server. You can configure DHCP on Windows Server 2012 R2 or on a Red Hat Linux server.

This section includes the following procedures:

- Configuring DHCP on Windows Server 2012 R2 on page 25
- Configuring DHCP on a Red Hat Linux Server on page 41

Configuring DHCP on Windows Server 2012 R2

Install DHCP either during the initial installation of Windows Server 2012 R2 or after the initial installation is completed.

DHCP options provide specific configuration and service information to DHCP clients. The options described here are specific to pointing an AP to its adopter and setting the correct MINT link level. The option value you configure is specific to your network site type.

When you configure DHCP for ExtremeCloud IQ Controller, include 078 SLP DA Option for access points on a Centralized site.

A scope is a collection of IP addresses meant to be distributed by the DHCP server to the client devices on a subnet.

Enable the DHCP Option for every scope you define. The DHCP Option is used by:

- The Wireless APs to discover the ExtremeCloud IQ Controller
- The mobility agents to discover the mobility manager.

Note
Go to http://support.microsoft.com for instructions on how to install DHCP.

Related Topics

Add a New DHCP Scope on page 26
Configure DHCP Server Options on page 32

Add a New DHCP Scope

Add a scope for the DHCP service.

To configure DHCP on Windows Server 2012 R2:

1. Select **Start** > **Administrative Tool** > **DHCP**.
2. In the console tree, right-click the DHCP server, IPv4 on which you want to create the new DHCP scope, and then select **New Scope**.
3. Select **Next**.
4. In the Name and Description text boxes, type the scope name and description.

   This can be any name that you want, but it should be descriptive enough so that you can identify the purpose of the scope on your network.

5. Select **Next**.

   The **IP Address Range** window is displayed.

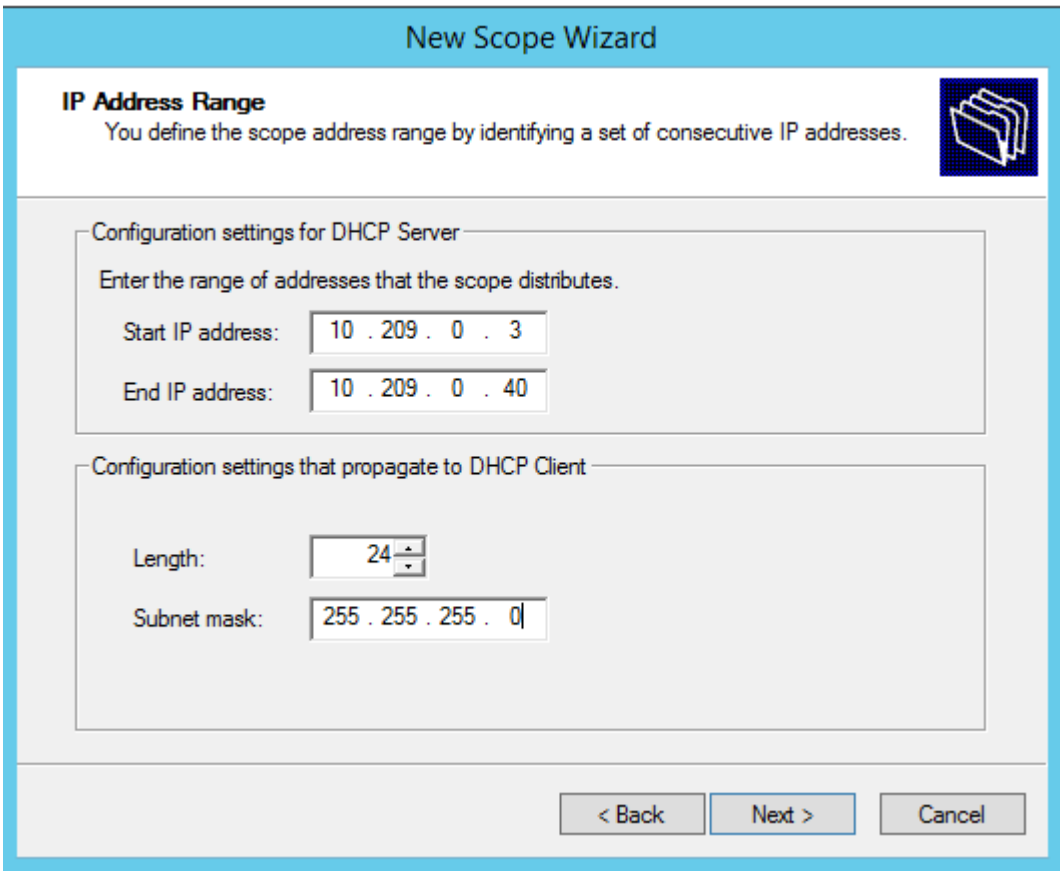


Figure 2: IP Address Range

6. In the Start IP address and the End IP address text boxes, type the start and end of the IP address range that you want to be distributed to the network.

   You must use the range provided by your network administrator.
7. In the Length text box, type the numeric value of the subnet mask bits, or in the Subnet mask text box, type the subnet mask IP address.

   A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address. You must use the Length (or the Subnet mask) provided by your network administrator.
8. Select **Next**.

   The **Add Exclusions** window displays.
9. In the Start IP address and the End IP address text boxes, type the start and end of the IP address range that you want to exclude from the distribution.

   You must use the exclusion range provided by your network administrator.

10. Select **Next**.

    The **Lease Duration** window displays.

    The DHCP server assigns a client an IP address for a given amount of time. The amount of time for which the IP address can be leased is defined in the Lease Duration window.
11. In the Days, Hours and Minutes text box, type the lease duration.

    You must use the Lease Duration as specified by your network administrator.
12. Select **Next**.

    The **Configure DHCP Options** window displays.
13. Select **Yes, I want to configure these options now**, and then select **Next**.

    The **Router (Default Gateway)** window displays.
14. In the IP address text box, type the network's default gateway and select **Add**.

    You must use the default gateway provided by your network administrator.

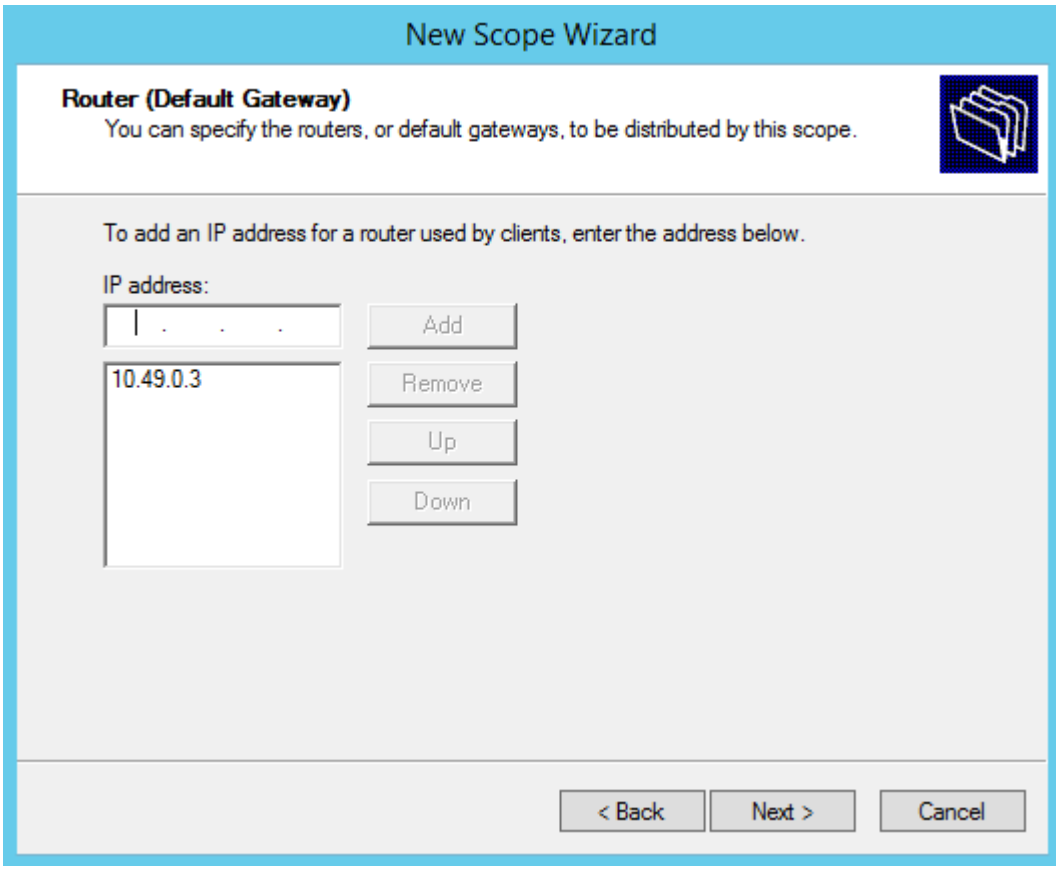


Figure 3: Router Default Gateway

15. Select **Next**.

    The **Domain Name and DNS Servers** window displays.

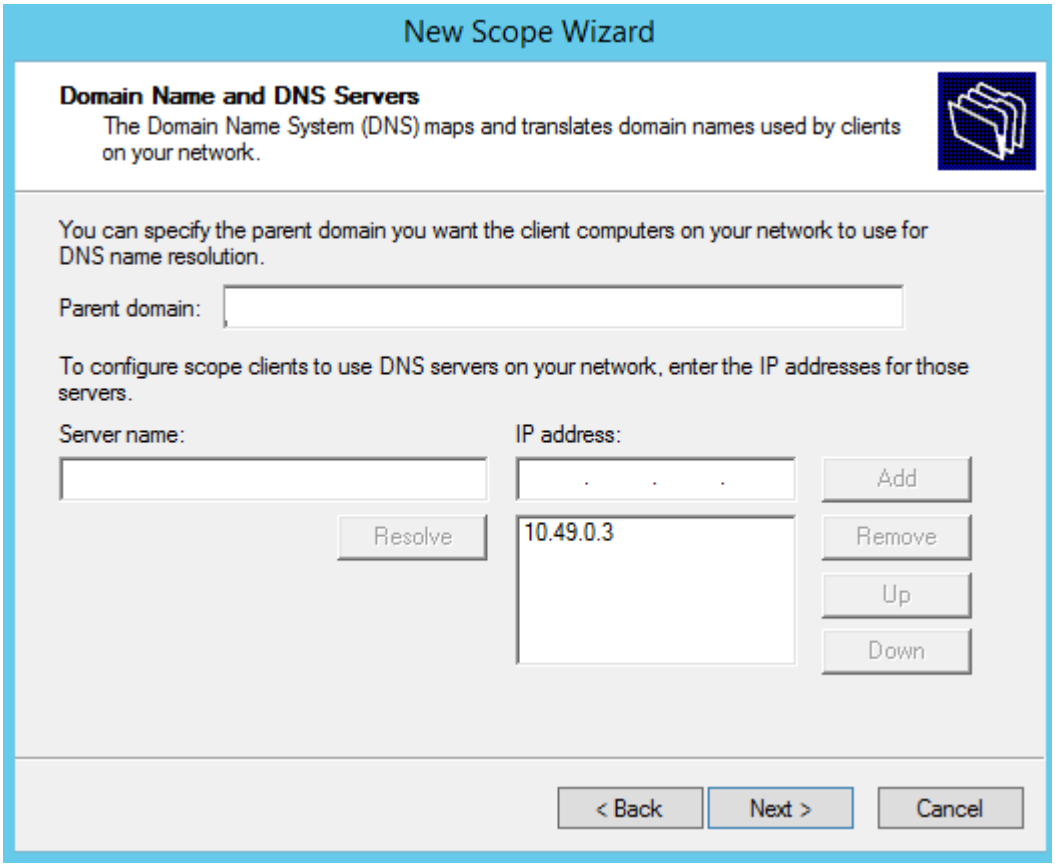


Figure 4: Domain Name and DNS Servers

16. In the Parent domain text box, type your company's domain name.

    You must use the Parent Domain provided by your network administrator.
17. In the Server name text box, type your server name.

    You must use the server name provided by your network administrator.
18. In the IP address text box, type your server's IP address, and then select **Add**.
19. Select **Next**.

    The **WINS Servers** window displays.
20. Select **Next**.

    The **Activate Scope** window displays.
21. Select **Yes, I want to activate this scope now**, and select **Next**.

    The wizard displays the following message:

    ```
    You have successfully completed the New Scope wizard.
    ```
22. Select **Finish**.

Related Topics

Create New DHCP Options on page 30

Create New DHCP Options

When you configure DHCP for ExtremeCloud IQ Controller, create 078 SLP DA Option for access points on a Centralized site.

Note
You can create the DHCP options at the scope level or at the server IPv4 node. When you configure DHCP options at the server node, the options apply to all scopes under that node.

Important
For AP deployments in remote locations where access points and controllers may need to be discovered and connected over firewalls, a best practice is to leverage DNS or DHCP Option 60/43 methods for zero-touch-provisioning discovery. These methods provide direct connectivity to the defined IP address. DHCP Option 78, which refers to the controller as a Service Location Protocol – Directory Agent (SLP-DA), requires the exchange of SLP protocol between the AP and the appliance at the core, necessitating that UDP 427 be allowed by any firewall in the path. For such installations, discovery over DHCP Option 78 assist is not recommended.

When using SLP, for an AP to establish connection with a controller, it must first exchange SLP Directory Agent registration before IPSEC establishment with the eventual controller. That means that SLP UDP 427 must be open along the path. Further issues can occur if Network Address Translation (NAT) is involved. While this method is popular and widely deployed within a homogenous campus, it may result in inadvertent complications for remote connections. Therefore, it should not be used in favor of an alternate method (DHCP 60/43 , DNS, or static override).

1. From the IPv4 node, right-click and select **Set Predefined Options**.
   The **Predefined Options and Values** dialog displays.
2. Option Class is **DHCP Standard Options**.
3. Select **Add**.
   The **Option Type** dialog displays.
4. Refer to the related information for each option.

Related Topics

Creating Option 78 on page 30
Configuring Option 43 on page 34

Creating Option 78

To create Option 78 for a Centralized site:

1. Go to **Start** > **Administrative Tool** > **DHCP**.
2. Right-click the server node, and select **Set predefined options**.
3. Select **Add**, and configure the following parameters:

   Name

   Provide a name for the option, for example **SLP DA**.

   Data Type

Set the data type to **Byte** and select the **Array** check box.

Code

78

Description

Optional description. For example, `Extreme Networks SLP Discovery`.

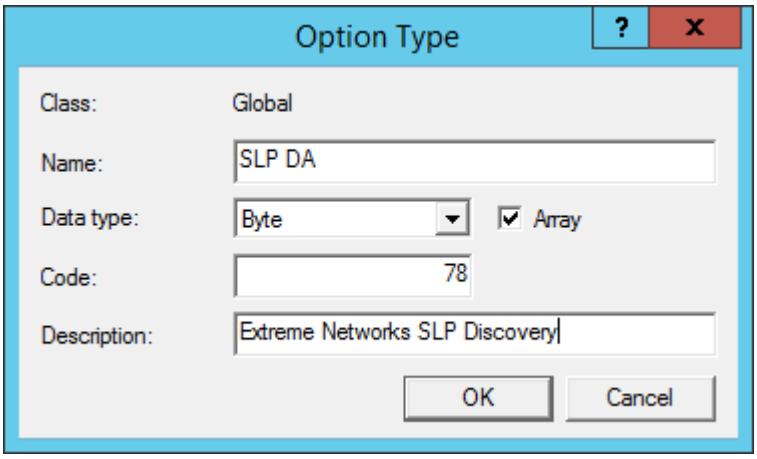


Figure 5: Option Type

4. Select **OK**.
5. Select **Edit Array** and enter the IP address per octet.

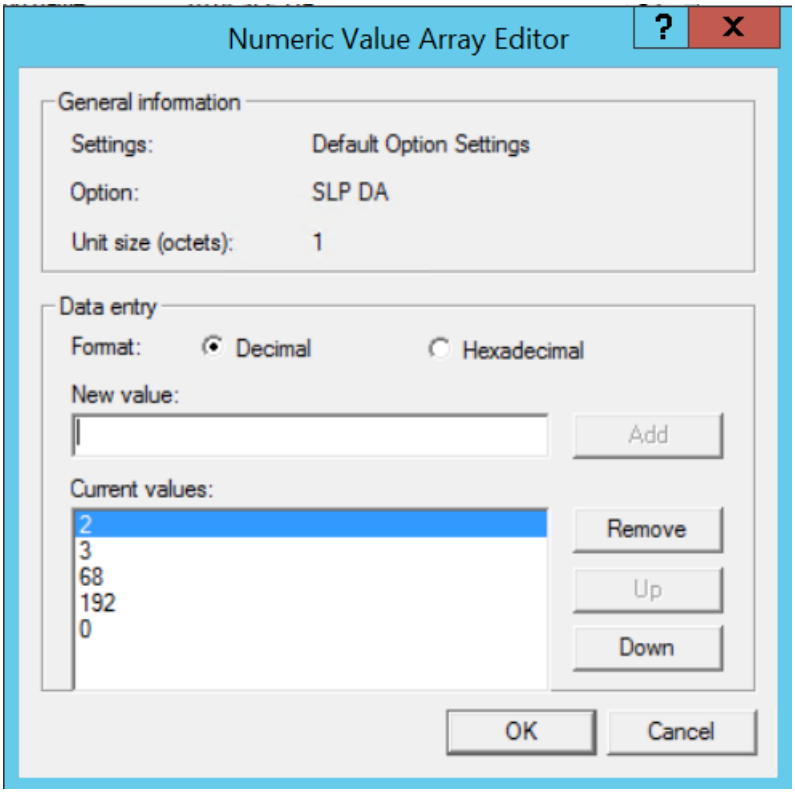


Figure 6: DHCP Option 78 Array Decimal Values

6. Select **OK**.

Related Topics

Configure DHCP Server Options on page 32

Configure DHCP Server Options

Configure the DHCP Option that you created under Create New DHCP Options on page 30. Configuring this option for the server, automatically includes the scope.

1. From the **IPv4** node, expand the tree.
2. Right-click **Server Options** and select **Configure Options**.

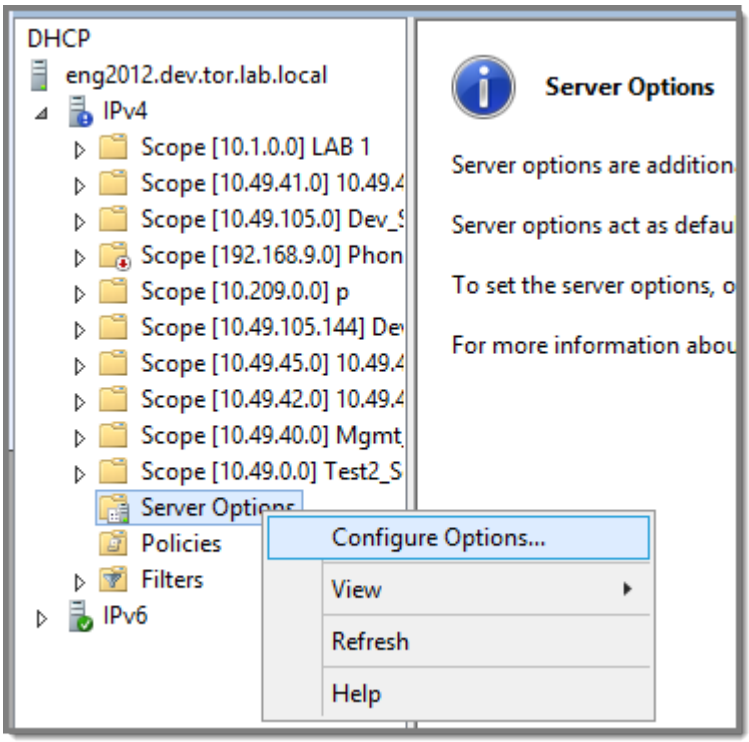


Figure 7: Configure Options

The **Server Options** dialog displays.

3. From the **General** tab, select the DHCP option you just created: 078 SLP DA

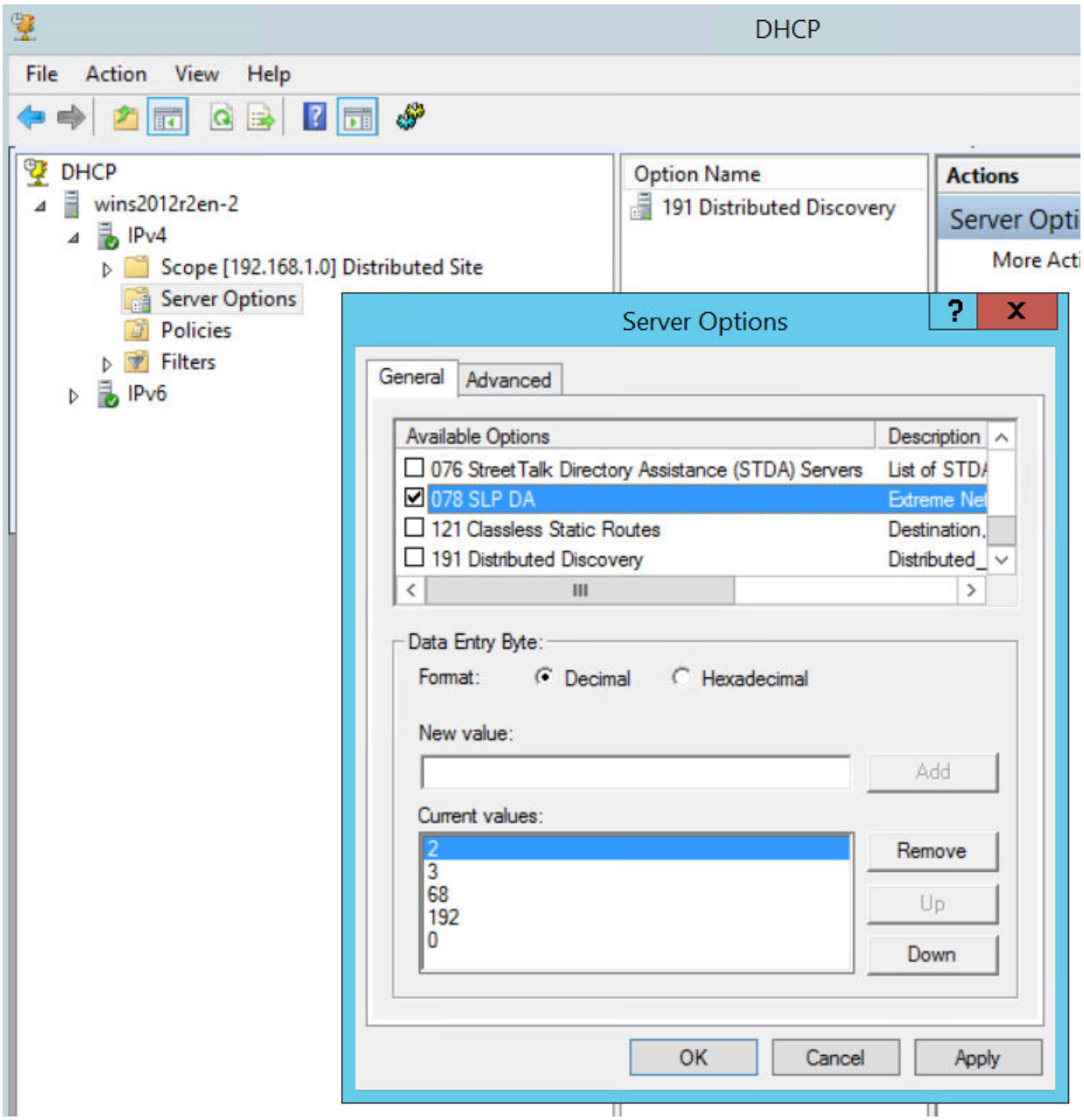


Figure 8: Configure Server Option 078

4. Verify the configured Data entry values for the selected option and select **OK**.

   In a Centralized site, the wireless APs use the SLP DA to discover the ExtremeCloud IQ Controller. The mobility agents use the SLP DA to discover the mobility manager. If there is no SLP deployment on the enterprise network, the ExtremeCloud IQ Controller is configured to act as a DA by default. If you put the appliance IP address in a DHCP server for Option 78, Wireless APs will interact with the appliance for discovery. Similarly, the mobility agents also interact with the ExtremeCloud IQ Controller to discover the mobility manager.

Related Topics

Creating Option 78 on page 30

Configuring Vendor Class on Windows Server 2012 R2

This section describes the Vendor Class Identifier on a Microsoft DHCP server for ExtremeCloud IQ Controller discovery. In the discovery process, the DHCP server returns vendor-specific information to the client. When an AP requests vendor specific information, the DHCP server sends the appliance IP addresses in Option 43 to the AP.

- Vendor Class Identifier (VCI)
  - The VCI for an ExtremeWireless AP39xx is `HiPath <AP model name>`. For example, the VCI for the ExtremeWireless AP3965e is `HiPath AP3965`.
  - The VCI for an ExtremeWireless 11ax AP is `WingAP.<AP model name>` . For example, the VCI for the ExtremeWireless AP505i is `WingAP.AP505` and AP410i is `WingAP.AP410`.
  - The VCI for the SA201 adapter is `HiPath SA201`.
- Option 43 sub-option code:
  - The option 43 sub-option code:
    - ExtremeWireless APs supported in a Centralized site is type 1 (0x1).
- IP addresses of ExtremeCloud IQ Controller.

Configuring Option 43

How to configure Option 43 on Windows Server 2012 R2.

Create Vendor Class

To create a vendor class using the Windows Server 2012 R2 DHCP, IPv4 server utility:

1. Go to **Start** > **Administrative Tool** > **DHCP**.
2. In the DHCP Server Utility, right-click the DHCP server icon and select **Define Vendor Classes**.

   You will create a new vendor class to program the DHCP server to recognize the VCI ExtremeWireless *<AP model name>*.

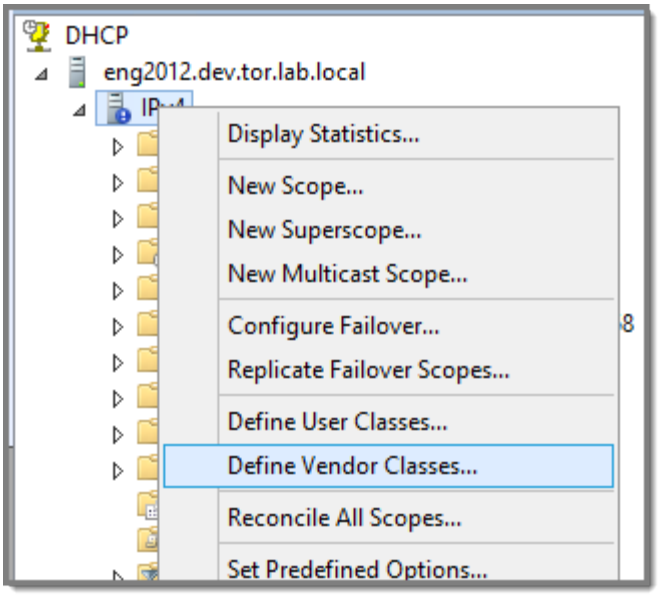


Figure 9: Define Vendor Classes

The **DHCP Vendor Classes** window displays.

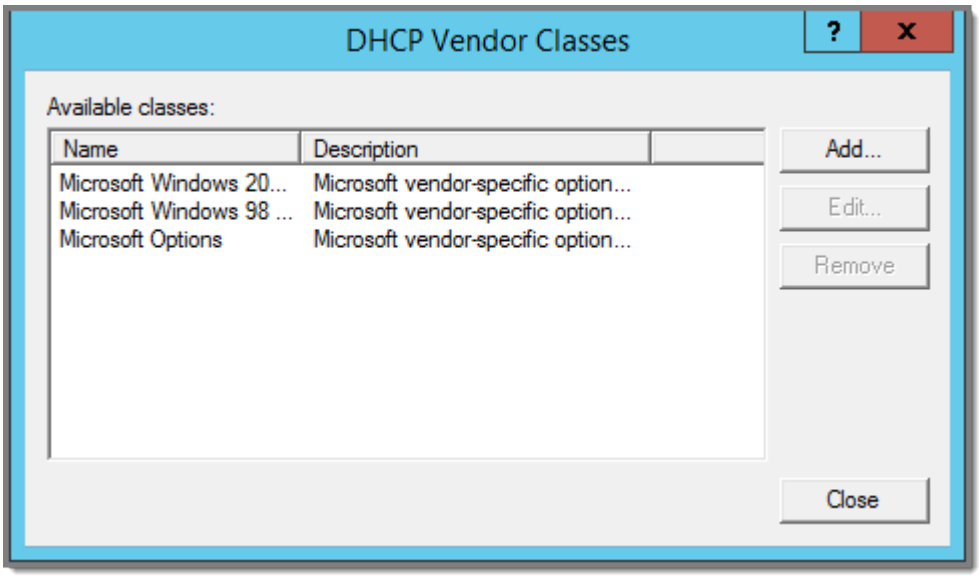


Figure 10: DHCP Vendor Classes

3. To create the new class, select **Add**.

   The **New Class** dialog displays.
4. Provide a Display Name and Description for the vendor class.

5. Select the ASCII field and type the VCI for the specific AP. For example, type **AP410** for an AP410i.

   The ID and Binary values are populated.

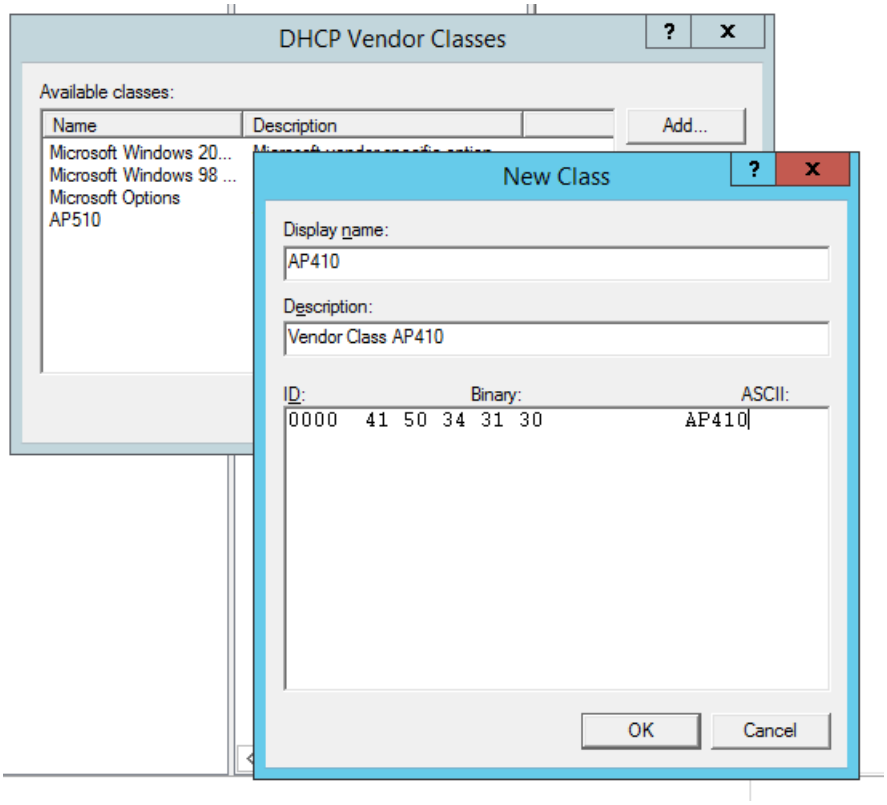


Figure 11: VCI AP410

6. Select **OK**.

   The new class is created.

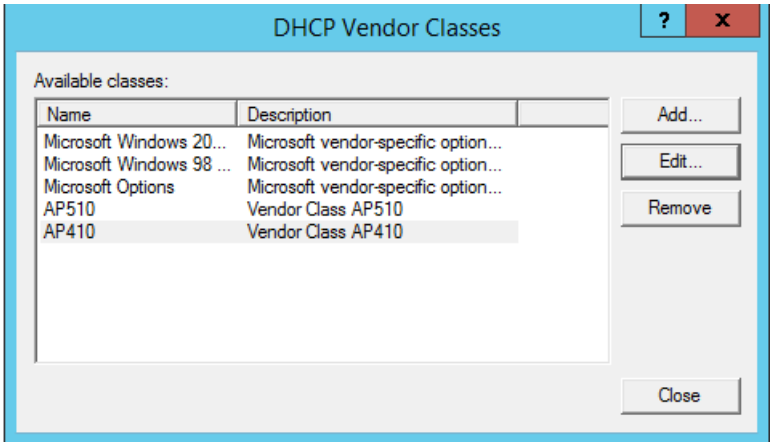


Figure 12: Vendor Classes

7. Select **Close**.

Configure Vendor Class

Configure the vendor class that you just created under Create Vendor Class on page 34.

1. Go to **Start** > **Administrative Tool** > **DHCP**.
2. In the DHCP server utility, right-click the server icon and select **Set predefined options**.

   Here we will add an entry for the WLAN controller sub-option for the newly created vendor class. The sub-option code type and the data format is used to deliver the vendor specific information to the APs.

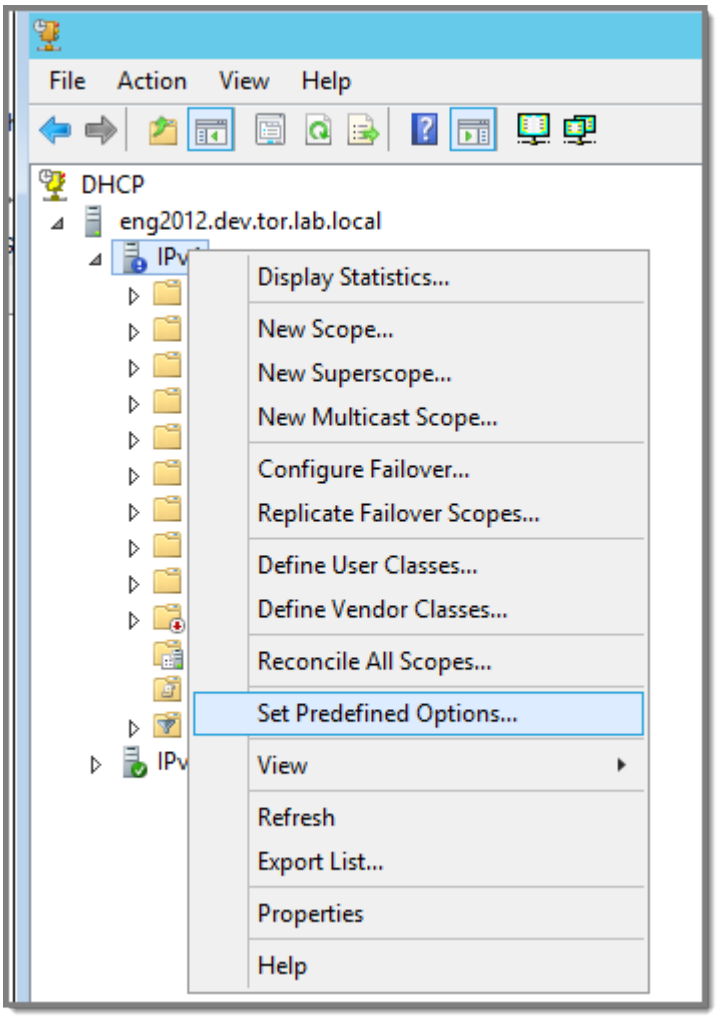


Figure 13: Set Predefined Options

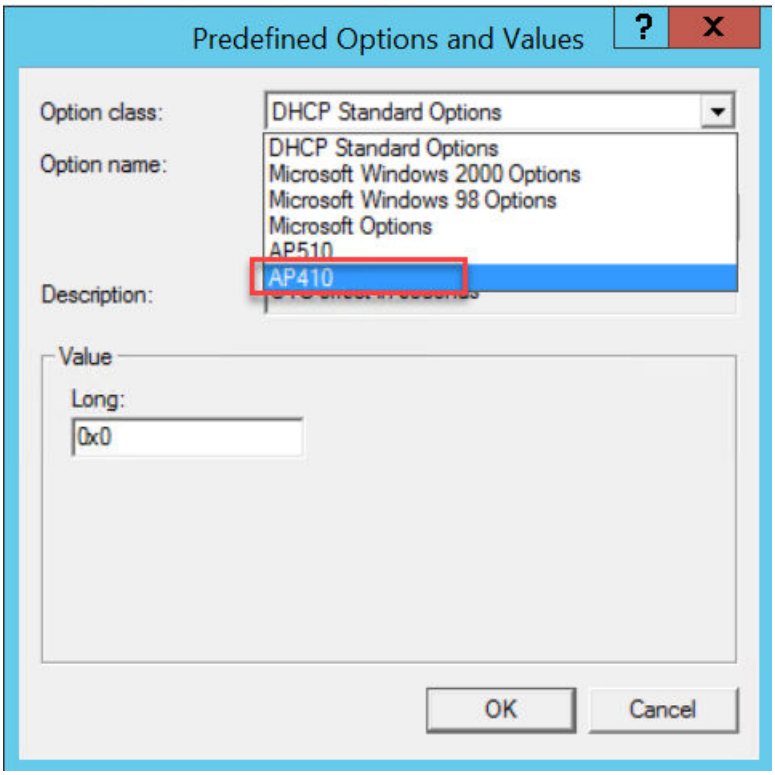


Figure 14: Predefined Options and Values

3. In the Option class field, select the value you configured for the vendor class and select **Add**.

   The **Option Type** window displays.

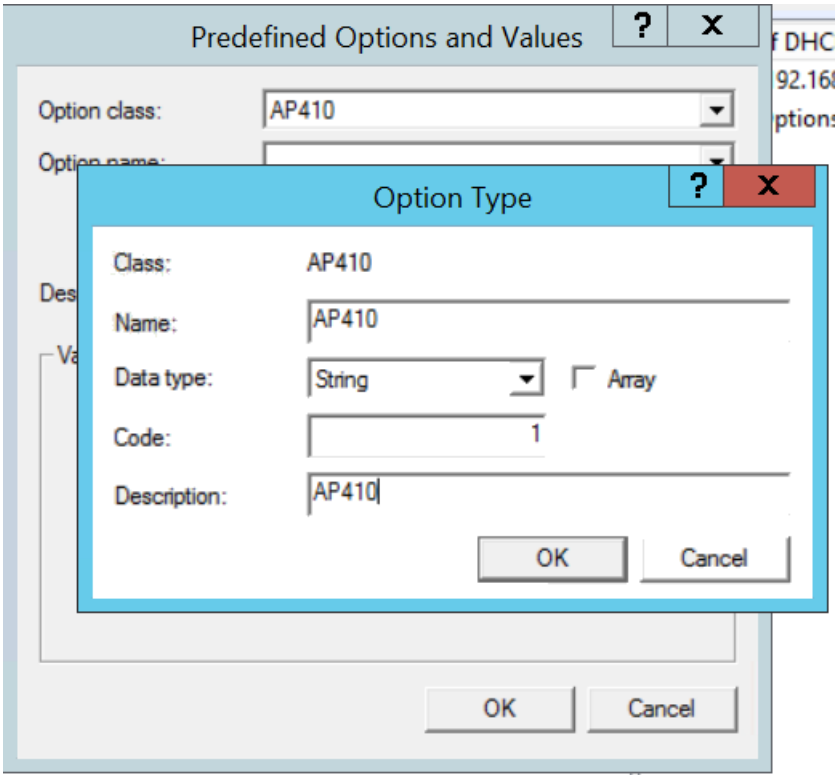


Figure 15: Option Type

4. Configure the following parameters:

   Name

   Name of the VCI option.

   Data Type

   Select **String**.

   Code

   Sub-option value **1**

   Description

   (Optional) Enter a description.

5. Select **OK**.

   The new predefined option is displayed in the **Predefined Options and Values** window.

6. Select **OK**.

   You have created the vendor class and sub-option type needed in order to support controller discovery.

Configuring Server Options

Associate the Vendor Class Identifier option with each DHCP scope.

1. In the DHCP server utility, right-click the **Server Options** folder under the DHCP scope, then select **Configure Options**.

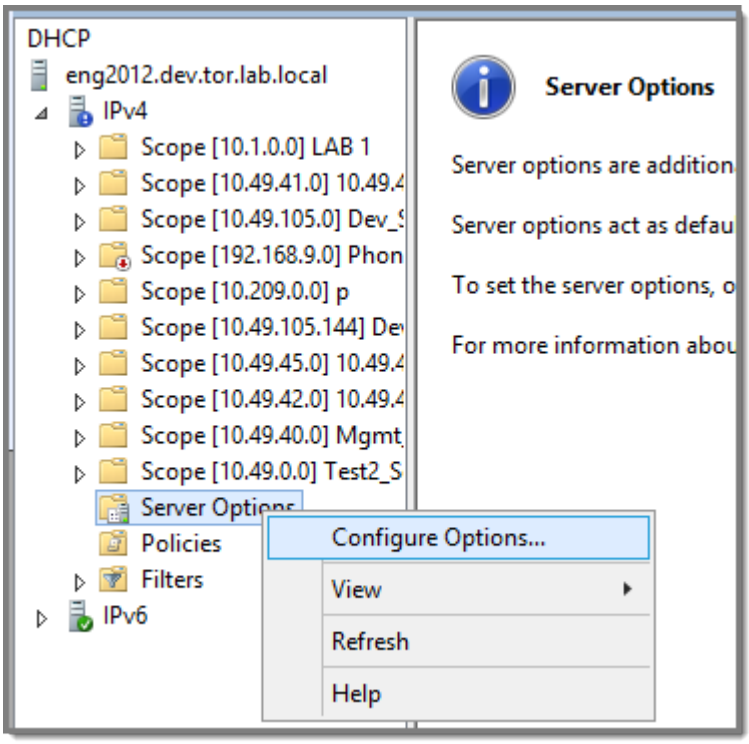


Figure 16: Configure Options

The **Scope Options** window displays.

2. Click the **Advanced** tab.

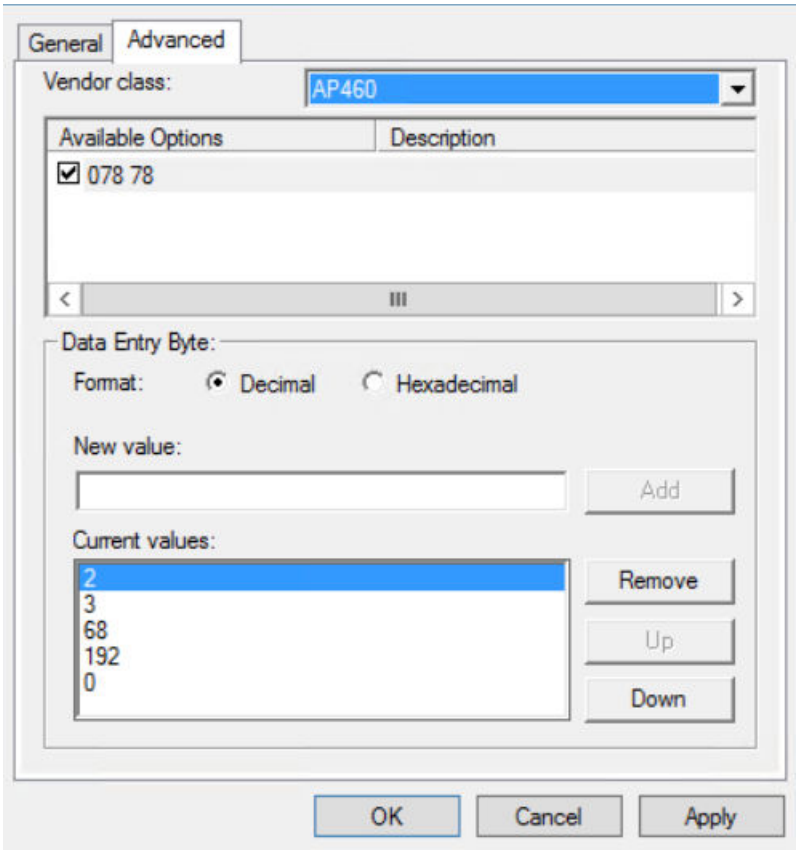


Figure 17: Vendor Class Option 078

Vendor Class

Select the vendor class that you plan to use. For example, AP410 or AP460.

Available Options

Select a predefined sub-option to assign to this scope. The option must be checked and highlighted to display Data Entry options.

Data Entry

(Option 078 Only) Enter the controller IP addresses to return to the APs. This is a comma-delimited list.

3. Click **OK**.

DHCP Option 43 is now configured. This DHCP option is available for all the DHCP scopes that are configured in the DHCP server. When an AP requests vendor specific information, the DHCP server sends the ExtremeCloud IQ Controller IP addresses in Option 43 to the AP.

Configuring DHCP on a Red Hat Linux Server

You can configure a DHCP server using the configuration file `/etc/dhcpd.conf`.

DHCP also uses the file /var/lib/dhcp/dhcpd.leases to store the client lease database.

The first step in configuring a DHCP server is to create the configuration file that stores the network information for the clients. Global options can be declared for all clients, or options can be declared for each client system.

The configuration file can contain any extra tabs or blank lines for easier formatting. The keywords are not case-sensitive and lines beginning with a hash mark (#) are considered comments.

To use the recommended mode, add the following line to the top of the configuration file:

```
ddns-update-style interim;
```

Read the dhcpd.conf man page for details about the different modes.

There are two types of statements in the configuration file:

- Parameters – State how to perform a task, whether to perform a task or what networking configuration options to use to send to the client.
- Declarations – Describe the Topology of the network, describe the clients, provide addresses for the clients, or apply a group of parameters to a group of declarations.

Some parameters must start with the option keyword and are referred to as options. Options configure DHCP options; whereas, parameters configure values that are not optional or control how the DHCP server behaves.

Parameters (including options) declared before a section enclosed in curly brackets {} are considered global parameters. Global parameters apply to all the sections below it.

Note
If you change the configuration file, the changes will not take effect until you restart the DHCP daemon with the command service dhcpd restart.

The following is an example of a DHCP configuration on a Red Hat Linux server.

For Wireless AP Subnet

```
subnet 10.209.0.0 netmask 255.255.255.0 {
option routers 10.209.0.2; ### This is the network’s default gateway address.
option subnet-mask 255.255.255.0
option domain-name xyznetworks.ca
option domain-name servers 192.168.1.3, 207.236, 176.11
range 10.209.0.3 10.209.0.40;
default-lease-time 7200000 ###The figures are in seconds.
## SLP option 78 for Extreme Wireless APs in a Centralized site.

option slp-directory-agent true 10.209.0.1, 10.209.0.3;

authoritative;
```

Configuring DHCP Option 43 on a Linux Server

This section describes the configurations necessary on the Linux DHCP server to use DHCP option 43 for ExtremeCloud IQ Controller discovery. Option 43 requires the following information:

- Vendor Class Identifier (VCI) — The VCI for an ExtremeWireless AP or adapter is HiPath <AP model name>. For example, the ExtremeWireless AP3912 is **HiPath AP3912** and the SA201 adapter is **HiPath SA201**.
- Option 43 sub-option code — The option 43 sub-option code for the ExtremeWireless APs is type 1 (0x1).
- IP addresses of ExtremeCloud IQ Controller

To configure the vendor encapsulated option on a Linux server, you must do the following:

- Define an option space.
- Define some options in that option space.
- Provide values for the options.
- Specify that this option space should be used to generate the vendor-encapsulated-options option.

To configure DHCP option 43:

1. Modify the dhcp.conf file (modifications are in bold).

```
[root@localhost ~]# vim /etc/dhcpd.conf
authoritative;
ddns-update-style interim;
ignore client-updates;
option space HAP;
option HAP.HWC code 1 = text;

subnet 10.100.1.0 netmask 255.255.255.0 {
range 10.100.1.10 10.100.1.254;
option subnet-mask 255.255.255.0;
option slp-directory-agent false 10.1.100.11;
option domain-name-servers 10.100.1.2;
option domain-name "bpmgmt.com";
option routers 10.100.1.1;
default-lease-time 40000;
}
…
subnet 10.100.4.0 netmask 255.255.255.0 {
range 10.100.4.100 10.100.4.254;
option subnet-mask 255.255.255.0;
option slp-directory-agent false 10.100.4.46, 10.100.4.47;
option domain-name-servers 10.100.1.2;
option domain-name "bpmgmt.com";
option routers 10.100.4.1;
default-lease-time 40000;


Vendor Class for ExtremeWireless APs:

class "HAP" {
match option vendor-class-identifier;
}
subclass "HAP" "AP3935" {
```

```
vendor-option-space HAP;
option HAP.HWC "10.100.2.36, 10.100.2.22";


}
```

2. Restart the DHCP server.

```
[root@localhost ~]# /etc/init.d/dhcpd restart
```

Configuring the ExtremeCloud IQ Controller as an NPS Client

1. Select **Start** > **Administrative Tools** > **Network Protocol Server**.
2. Expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and then select **New**.
3. Configure the following parameters:
   - Friendly name. Type the name that you want to assign to the ExtremeCloud IQ Controller
   - Client address (IP or DNS). Type the IP address of the ExtremeCloud IQ Controller, and then select **Verify**.

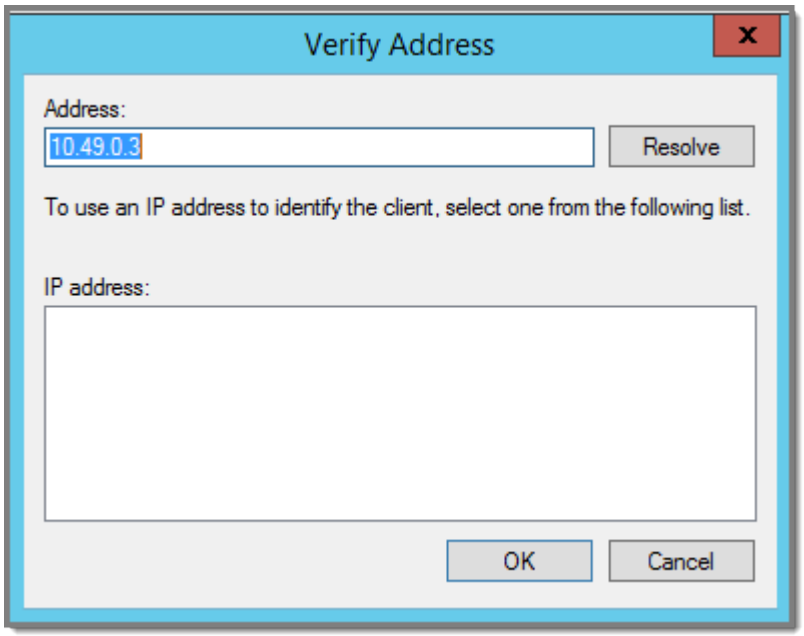


Figure 18: Verify Address

   a. Select **Resolve**.

      If the IP address is correct, it displays in the Search results text box.

   b. Select **OK**.

   - Shared Secret. Select a Shared Secret Template (Optional).

You can opt to enter a Shared Secret manually or have NPS generate the Shared Secret.

- Manual. Type a password that both the NPS server and the ExtremeCloud IQ Controller will use to mutually authenticate. This password is case-sensitive. You can use alpha-numeric characters. You must configure the same shared secret password for the VNS .
- Generate. Select **Generate** to have NPS generate the password. Not all servers support long generated secrets.

4. Select **OK**.

NPS Service Configuration

Microsoft Network Policy Server (NPS) can run as a RADIUS server. You can use NPS for centralized authentication and accounting of multiple client devices. To install NPS on Windows Server 2012 R2, see http://support.microsoft.com. This section outlines the following configuration procedures:

- Add a New Network Policy on page 45
- Configuring the ExtremeCloud IQ Controller as an NPS Client on page 44

Add a New Network Policy

Create one or more network policies. In this section, we outline how to create two specific policy conditions. Adding policy conditions is optional.

- Create a condition to limit the policy to specific IP addresses.
- Create a condition to limit the policy to a specific group that corresponds to an ExtremeCloud IQ Controller Role.

To create a new network policy:

1. Select **Start** > **Administrative Tool** > **Network Policy Server**.
2. In the tree view, expand **NPS (Local)**, expand **Policies**, and right-click **Network Policies**.
3. Select **New**
4. Provide a **Policy name**.
   - Type of network access server is **Unspecified**.
   - Do not select **Vendor Specific**
5. Select **Next** to configure a condition if applicable.

Related Topics

Create Condition: Client IPv4 Addresses on page 45
Create Condition: Windows Groups on page 47

Create Condition: Client IPv4 Addresses

1. Select **Add** to add a condition.
2. Scroll down to Radius Client Properties and select **Client IPv4 Addresses**.

3. Enter the IP Address of the ExtremeCloud IQ Controller and select **OK**.

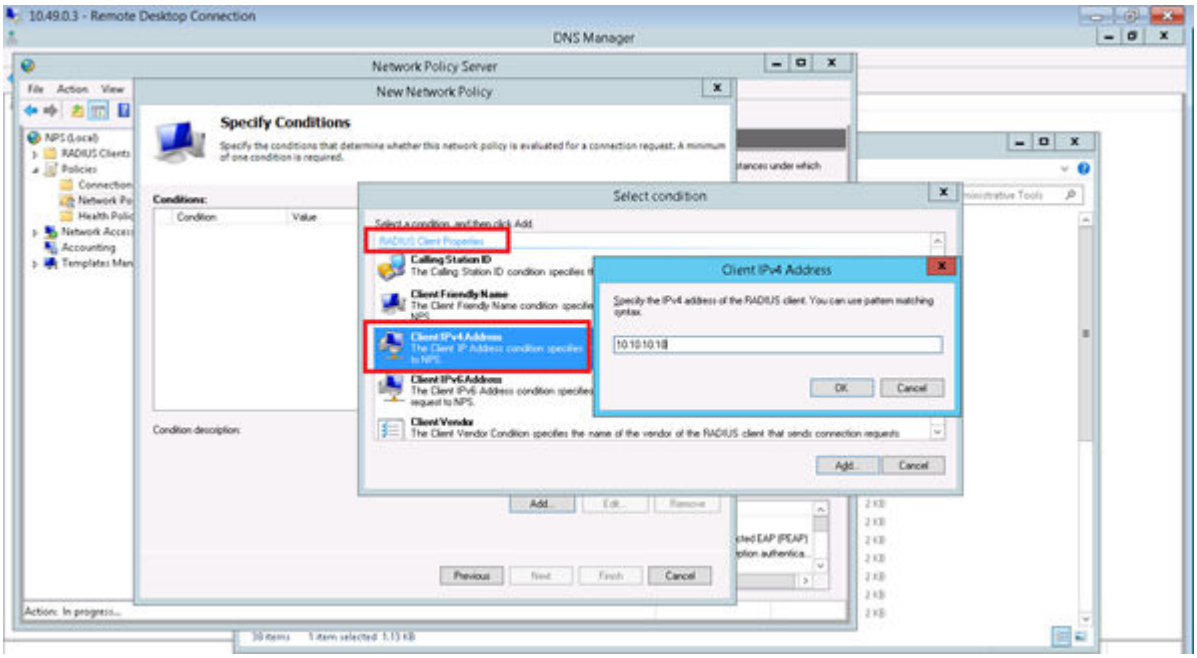


Figure 19: Condition: Client IPv4 Address

4. Select **Next**.
5. On the **Specify Access Permission** screen, select **Access granted** and select **Next**.
6. On the **Configure Authentication Methods** screen, select **Add** and select **Microsoft: Smart Card or other certificate**. Then, select **OK**.

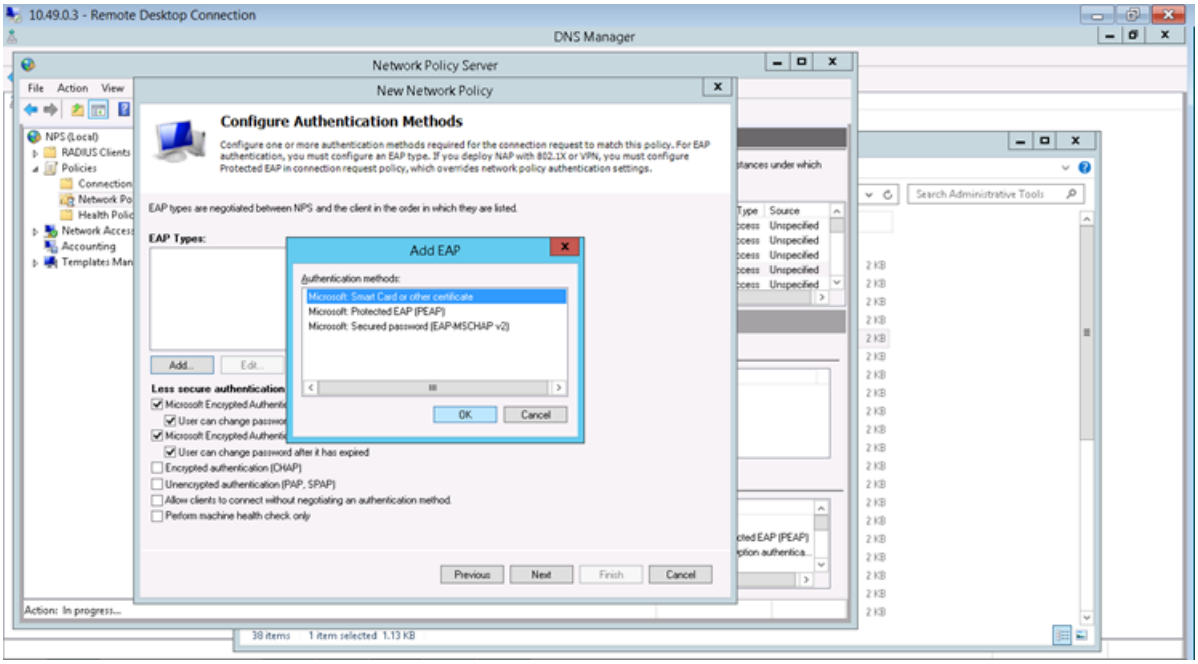


Figure 20: Add EAP

7. Select **Next**.

8. Configure the Idle Timeout and select **Next**.
9. Configure the Radius Attributes and select **Next**.
10. Select **Finish**.

Create Condition: Windows Groups

Create a condition specifying a Windows group to add flexibility to policy management.

1. Select **Add** to add a condition.
2. Select **Windows Groups** and Select **Add**.
3. Select **Add Groups**.

   The **Select Group** dialog opens.

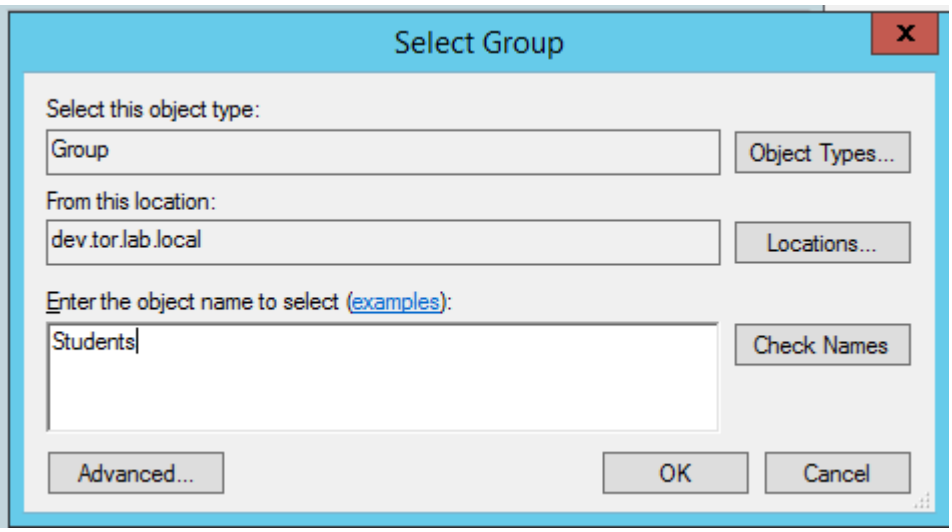


Figure 21: Select Group

4. Type `Group` as the object type.
5. Specify the location.
6. Enter the name of the group. This name must match a configured Active Directory group. You may be prompted to specify the Active Directory Windows group that the group corresponds to.
7. Select **OK**.
8. On the **Specify Access Permission** screen, specify the level of access permission and select **Next**.

9. On the **Configure Authentication Methods** screen, select **Add** and select one or more EAP methods. Then, select **OK**.

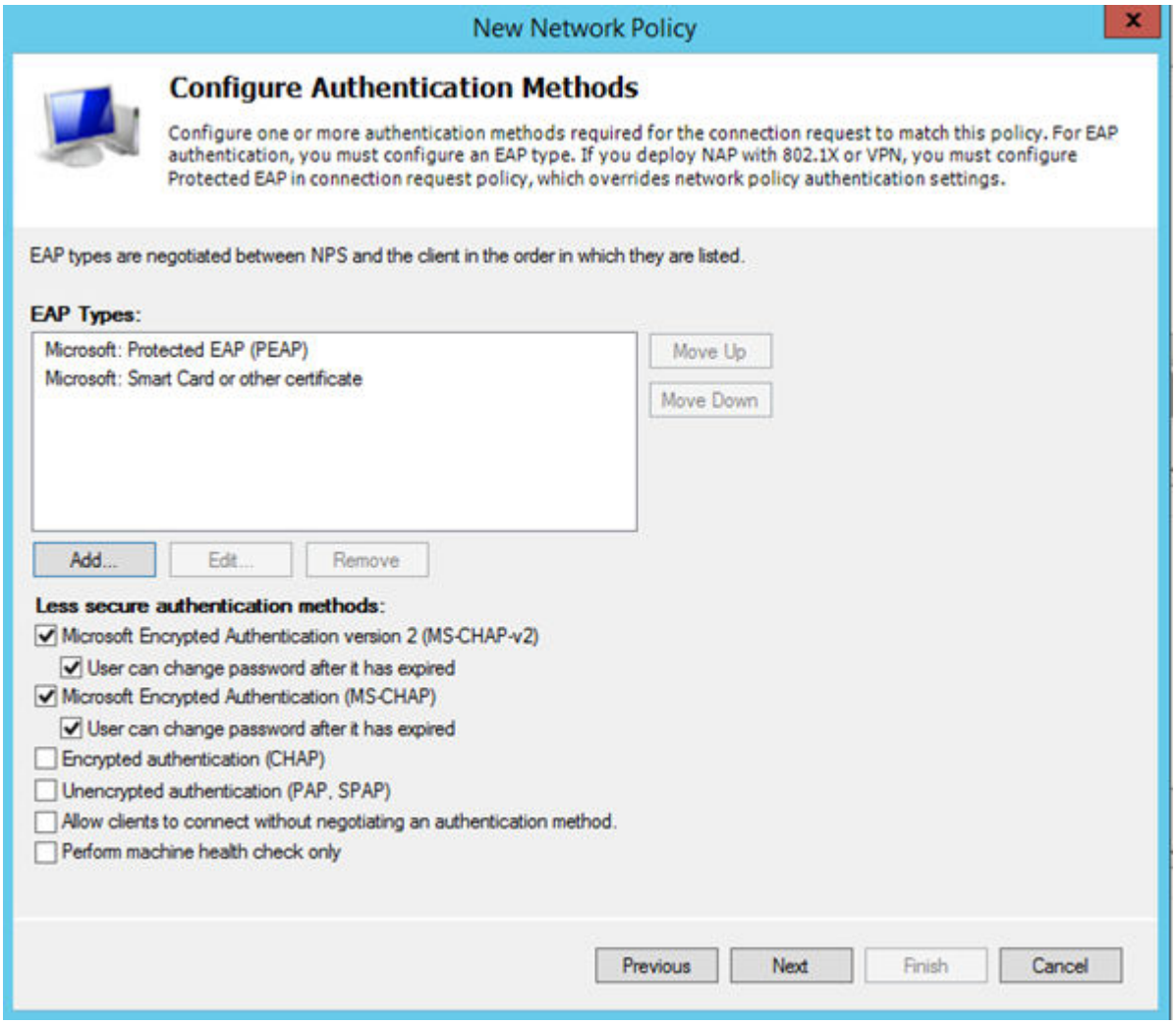


Figure 22: Configure Authentication Methods

10. Select **Next**.
11. Configure the Idle Timeout and select **Next**.
12. Configure the Radius Attributes. As an example, you can set the Filter-Id attribute to a wireless controller role. This will override the default role. The following procedure illustrates how to set the Filter-Id:
13. Select **Add**, select the **Filter-Id** attribute.
14. Select **Add**.

15. Select **Add** again and type the attribute name. The Attribute name is case sensitive and must match the Role on the wireless controller.

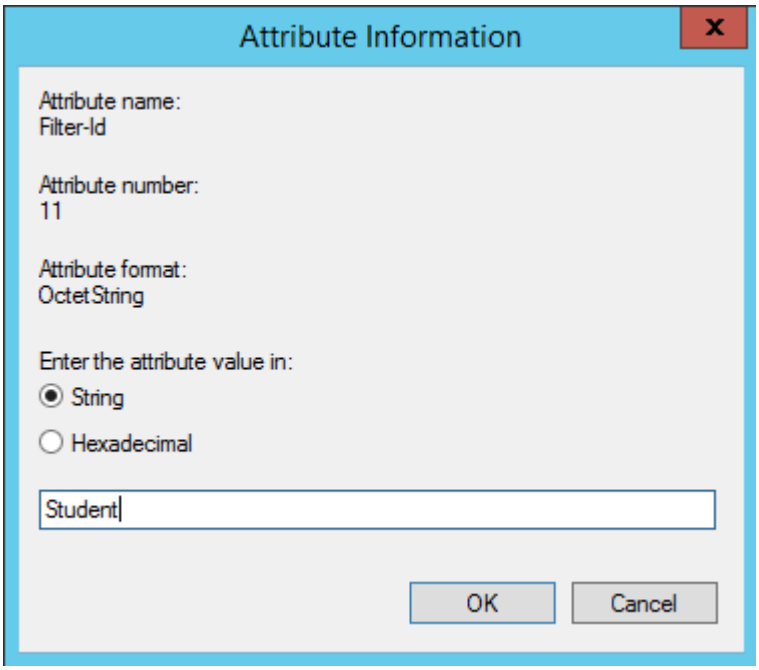


Figure 23: Attribute Information

16. Select **OK**.
17. Select **Close** to close the **RADIUS Attribute** dialog.

18. Select **Next**.

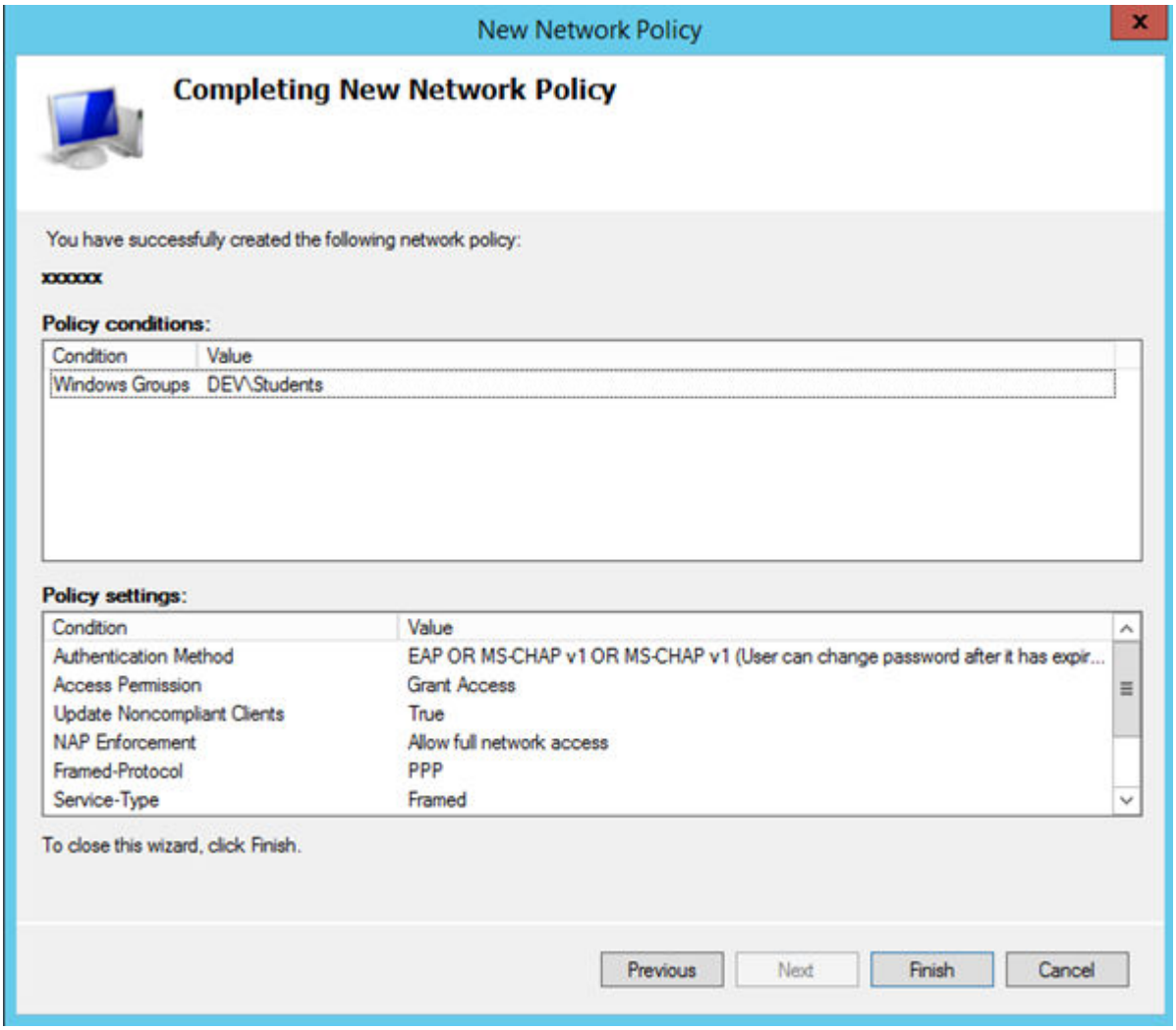


Figure 24: Completing New Network Policy

19. Select **Finish**.

DNS Service Configuration

The domain name system (DNS) stores and associates many types of information with domain names, but most importantly, it translates domain names (computer hostnames) to IP addresses.

You must install DNS on Windows Server 2012 R2 according to the server documentation. Visit http://support.microsoft.com to learn how to install and configure DNS on Windows Server 2012 R2.

The instructions here are limited to Configuring DNS for Wireless APs Discovery.

For configuration on Linux, see Configuring DNS on a Linux Server on page 52.

Configuring DNS for Wireless AP Discovery

1. Click **Start** > **Administrative Tools** > **DNS** .
2. Expand the tree and right-click on a domain.
3. Select **New Host (A or AAA)**.

   The **New Host** window displays.

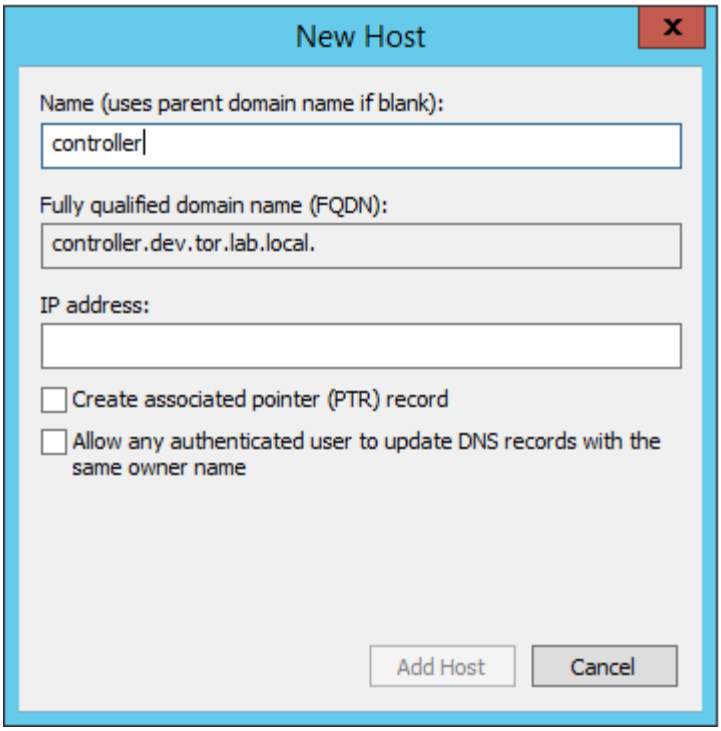


Figure 25: New Host

4. In the Name text box, type *controller*
5. In the IP address text box, type the ExtremeCloud IQ Controller IP address.

   If configuring multiple controllers, create all records with the same name controller, and provide unique IP addresses.
6. Select **Create associated pointer (PTR) record** check box.

   This option creates a record for reverse lookup.

   Note
   ExtremeWireless WiNG APs — Use a Domain Name Server (DNS) lookup for the host name `Controller.<domain-name>`. If you use this method for discovery, place an `"A" record` in the DNS server for Controller.<domain-name>. The <domain-name> is optional, but if used, ensure it is listed with the DHCP server.

7. Click **Add Host**.

   The new host is displayed in the right pane of the screen.
8. Click **Done**.

You must now configure the Wireless APs via the ExtremeCloud IQ Controller.

Configuring DNS on a Linux Server

This section describes the procedure to configure Linux DNS server for ExtremeCloud IQ Controller IP addresses discovery.

1. Configure the Linux DHCP server to include DNS information. In the `/etc/dhcp.conf` file, add domain-name-servers and domain-name DHCP options.

```
subnet 10.2.221.0 netmask 255.255.255.0 {
range 10.2.221.30 10.2.221.130;

option slp-directory-agent true 10.2.221.2;
option subnet-mask 255.255.255.0;
option domain-name-servers 192.168.6.2;
option domain-name "Availability-221.com";
option routers 10.2.221.1;
default-lease-time 40000;
}
```

2. Configure the Linux DNS server to include ExtremeCloud IQ Controller IP addresses.

   Create a file for the domain name configured in dhcp.conf (in this example, "Availability-221.com") as follows at `/var/named/chroot/var/named`.

   The name of the file should be the following: `/var/named/chroot/var/named/named.Availability-221.com`

```
/var/named/chroot/var/named/named.Availability-221.com
$TTL 86400
@     IN    SOA   ns1.availability-221.com.     hostmaster.availability-221.com.    (
                            2      ; serial #
                            28800   ; refresh
                            14400   ; retry
                            3600000 ; expire
                            86400   ; ttl
                            )
                IN    NS    ns1.availability-221.com.
Controller      IN    A     10.2.221.2
```

3. Add the domain name to the DNS configuration file (`/var/named/chroot/etc/named.conf`).

```
$//
// a caching only nameserver config
//
options {
/*
 * If there is a firewall between you and nameservers you want
 * to talk to, you might need to uncomment the query-source
 * directive below.  Previous versions of BIND always asked
 * questions using port 53, but BIND 8.1 uses an unprivileged
 * port by default.
 */
// query-source address * port 53;
version "Bind";
recursion no;
directory "/var/named";
};
zone "Availability-221.com" {
       type master;
       file "named.Availability-221.com";
};
zone "0.0.127.in-addr.arpa" {
type master;
```

```
file "named.local";
allow-update { none; };
```

4. Confirm that DNS service is running.

```
ps -ef | grep named
named 10023 1 0 Feb18 ? 00:00:00 /usr/sbin/named -u named -t /var/named/chroot
root 7687 7531 0 22:14 pts/982 00:00:00 grep named
```

5. Verify that the domain name is configured properly.

```
nslookup Controller.Availability-221.com
Server:            127.0.0.1
Address:           127.0.0.1#53

Name:  Controller.Availability-221.com
Address: 10.2.221.2
```

Configure ExtremeCloud IQ Controller for Local DHCP Management

For Bridged@AC configurations, the appliance can be configured as a Local DHCP (Dynamic Host Configuration Protocol) server for the VLAN segment. This is useful for deployments that do not have access to an infrastructure provided DHCP server. Configure ExtremeCloud IQ Controller as a Local DHCP from the **Layer 3** settings of a Bridged@AC topology.

When the appliances are configured as a High Availability pair, the configuration sync to the peer appliance results in two DHCP servers being configured for one appliance pair. ExtremeCloud IQ Controller automatically syncs the configuration for redundancy. Therefore, if one appliance (and its corresponding DHCP server instance) is removed, the remaining appliance (and DHCP server) have full visibility of the allocated DHCP set, and support the subnet without interruption or conflict.

When configuring ExtremeCloud IQ Controller for providing IP addresses to APs, take the following steps on both appliances in a High Availability Pair:

1. Define a physical topology on each ExtremeCloud IQ Controller.

   Configure a shared subnet and a unique IP address for each controller.
2. From ExtremeCloud IQ Controller, enable **Local DHCP server** on the physical topology for both controllers.
3. Specify the same L2 subnet on both physical topologies. The following settings should match on both controllers:

   Ensure that the following Physical Interface Settings match on both appliances in the High Availability Pair:
   - Mode
   - VLAN ID
   - Tagged
   - Port
   - Device Registration
   - Traffic Management

Endure that the following Local DHCP settings match on both appliances in the High Availability Pair:

- Gateway IP address
- IP Address Range

Related Topics

Add a Physical Interface on page 54
Local DHCP Settings on page 55

Add a Physical Interface

Note
You must be a system administrator to add a network interface.

Take the following steps:

1. Go to **Administration** > **System**.
2. Under Interfaces select **Add**.

   The **Create New Interface** dialog displays.
3. Configure the following parameters:

Table 8: Interface Parameters

Field	Description
Name	Name of the interface.
Mode	Physical - The topology is the native topology of a data plane and it represents the actual Ethernet ports.
VLAN ID	ID for the virtual network.
Tagged	Indicates if the interface tags traffic. When traffic is tagged, the VLAN ID is inserted into the packet header to identify which VLAN the packet belongs to. Tagging can identify the port or interface to send a broadcast message to.
Port	Physical port on the ExtremeCloud IQ Controller for the interface.
Enable Device Registration	Enable or disable AP registration through this interface. When enabled, wireless APs use this port for discovery and registration. Other ExtremeCloud IQ Controllers can use this port to enable inter-ExtremeCloud IQ Controller device mobility if this port is configured to use SLP or the ExtremeCloud IQ Controller is running as a manager and SLP is the discovery protocol used by the agents.
Management Traffic	Enable or disable Management Traffic through this interface. Enabling management provides access to SNMP (v1/v2c, v3), SSH, and HTTPs management interfaces.

Table 8: Interface Parameters (continued)

Field	Description
MTU	Maximum Transmission Unit (MTU). Standard is 1500 bytes. Fixed value.
Layer 3	
IP Address	For an Admin topology, the Layer 3 check box is selected automatically. The IP address is mandatory for a Physical topology. This allows for IP Interface and subnet configuration together with other networking services.
CIDR	CIDR field is used along with IP address field to find the IP address range.
FQDN	Fully-Qualified Domain Name
DHCP	Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses. Valid values are: • None • Local Server. Indicates that the ExtremeCloud IQ Controller is used for managing IP addresses.

Related Topics

Local DHCP Settings on page 55

Local DHCP Settings

Configure the following Local DHCP settings:

Domain Name

The name of the domain that is allocated for the IP address range.

Lease (Seconds)

The DHCP Lease represents the time period between when a device obtains the IP address and the time the IP address expires. When the **Lease** expires, the device releases the IP address and ExtremeCloud IQ Controller issues a new one. Default Lease is 36000 seconds, Default Max Value is 2592000 seconds. Devices can request a lease value.

DNS Servers

Primary IP address for the DNS (Domain Name Server).

WINS Servers

IP address of the WINS (Windows Internet Name Service) server.

Gateway

Gateway IP address.

Address Range

IP address range. Value is prompted by the subnet IP address that you configured.

Exclusions

(Available from the VLAN configuration) A range or single IP address that is excluded from the greater Address Range. Save your VLAN configuration before selecting **Exclusions** to configure IP address exclusions.

Centralized Site with an Internal Captive Portal

Adding a Centralized Site with Device Group on page 57
Configuring an Internal Captive Portal on page 59
Specifying B@AC Network Topology on page 60
Configuring a Captive Portal Network on page 61
Working with Internal Captive Portal Engine Rules on page 62
Editing Device Group Profile for Network and Role on page 63
Creating Adoption Rules on page 65

Deployment Strategy

The following strategy outlines how to create a Centralized site with an internal captive portal:

1. Add a Centralized site with a device group.
2. Configure an internal captive portal.
3. Specify a network topology.
4. Configure a captive portal network.
5. Work with engine rules.
6. Specify the network and role in the device group profile.
7. Create adoption rules.

Adding a Centralized Site with Device Group

Before you create a site, know the following information about your network:

- AP licensing domain
- AP models.

For this deployment scenario, the licensing domain is ROW (Rest of World).

For this deployment scenario, the AP model is AP3915.

1. Go to **Configure** > **Sites** > **Add** and configure the following parameters:

   Name

   Site_Row

   Country

   Select **Toronto Canada**.

This value corresponds to the licensing domain ROW.

Timezone

Canada: America/Toronto

2. Create one or more device groups for the site.

   All APs in a device group must share the following:

   - AP model number
   - Configuration Profile
   - RF Management Profile

   Go to **Configure** > **Sites** and select a site. Then, select **Device Groups** > **Add** and configure the following parameters:

   Name

   DeviceGroup_AP3915

   Profile

   AP3915-default

   Select a configuration profile for the AP model. The configuration profile is specific to the AP model.

   RF Management

   Select **Default ACS**.

   This option displays after you have selected the configuration profile, because the RF Management options depend on the selected configuration profile. A Centralized site supports the following AP models:

   - AP39xx supporting ACS Policy for RF Management
   - AP3xx, AP4xx, AP5xx.

   Note

   AP4xx and AP5xx currently require manual channel plan configuration when used in a Centralized site. Go to **Configure** > **Devices** > **Access Points** and select an AP5xx model. For more information, see *Configure AP Radio Settings* in the *User Guide*

3. Select from the list of discovered APs.

   Auto-discovered APs that match the selected configuration profile display in a list on the **Create Device Group** dialog.

4. Click **OK**.

Figure 26: Create Device Group AP3915

5. Click **Save** on the **Site** page to save the site and device group.

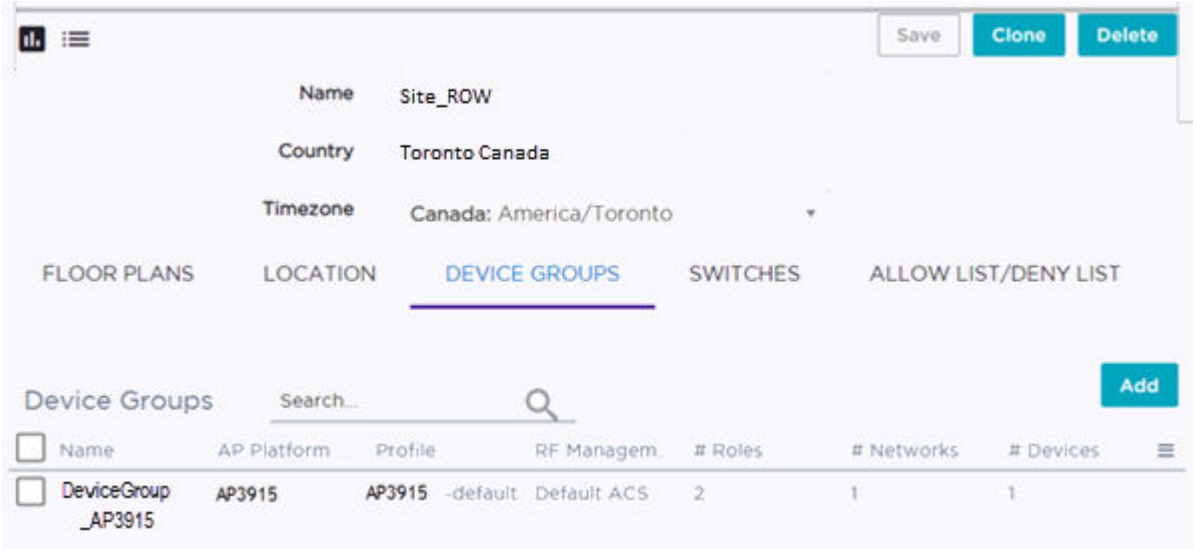


Figure 27: Centralized Site with One Device Group

Next, configure an internal captive portal.

Related Topics

Configuring an Internal Captive Portal on page 59

Configuring an Internal Captive Portal

Creating a captive portal on ExtremeCloud IQ Controller that is authenticated with an external RADIUS server.

1. Go to **Onboard** > **Portal** > **Default** and select the portal type.
2. From the Authenticated Portal field, select **Authenticated Web Access** and click **Save**.

3. Go to **Onboard** > **AAA** > **RADIUS Servers** > **Add** and configure the following parameters for your RADIUS server.

   RADIUS Server IP address

   Valid IP address of the RADIUS server.

   Shared Secret

   Password for the RADIUS server. The value must be at least six characters.
4. Click **Save**.

Next, specify a network topology.

Related Topics

Specifying B@AC Network Topology on page 60

Specifying B@AC Network Topology

ExtremeCloud IQ Controller offers a default VLAN that is Bridged@AP, untagged. Each site can only have one untagged VLAN. For this deployment, we will specify Bridged@AC topology.

1. Go to **Configure** > **Policy** > **VLANS** > **Add** and configure the following parameters:

   Name

   test1

   Mode

   Bridged@AC

   VLAN ID

   Specify a valid VLAN ID.

   Port

   If the Mode is Bridged@AC, specify a data port.

   Layer 3

   If the Mode is Bridged@AC, provide the following Layer 3 parameters:

   - IP Address
   - CIDR
   - FQDN
   - DHCP.

     Select **Relay**, then click **Configure** to enter the DHCP Relay Server IP address.
   - Enable Device Registration. Indicates that the wireless AP or switch can us this port for discovery and registration.
   - Mgmt traffic. Indicates that this port will be used to manage traffic. Enable **Mgmt Traffic** to access the ExtremeCloud IQ Controller user interface through this port.
2. Click **Save**.

Next, add a network.

Related Topics

Configuring a Captive Portal Network on page 61

Configuring a Captive Portal Network

Configuring an Internal Captive Portal network with WPAv2 PSK privacy.

Note
Centralized sites support B@AC and B@AP VLAN topology.

1. Go to **Configure** > **Networks** > **WLANs** > **Add** and configure the following parameters:

   Network Name

   test1-ICP

   SSID

   test1-ICP

   Status

   Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

   Auth Type

   Select **WPAv2 - Personal (PSK)** then select **Edit Privacy** and enter a password key.

   Enable Captive Portal

   Check this option and specify the following parameters:

   - Captive Portal Type = **Internal**
   - **Default** captive portal is specified. This is the captive portal we configured.
   - Authentication Method. Select **Proxy RADIUS (Failover)**.

     Note
     Policy assignment through Filter ID is not supported.

   - Primary RADIUS. This is the RADIUS server we configured. Enter the IP address. You have the option to add 1-3 failover RADIUS servers.
   - Default VLAN = **test1**. This is the B@AC VLAN we created.

   Default Auth Role

   The default network policy roles for an authenticated client. Select the plus sign to create a new role.

   Select the policy role as the default authentication policy role. Typically, **Enterprise User** is the Default Auth Role. You can select any of the configured roles.

   To configure a new role:

   a. Go to **Configure** > **Policy** > **Roles**.

b. Go to **Onboard** > **Rules** and edit a policy rule, specifying **Default Auth Role** in the Accept Policy field.

Default VLAN

The default network topology. A topology can be thought of as a VLAN (Virtual LAN) with at least one egress port, and optionally include: sets of services, exception filters, and multicast filters. Examples of supported topology modes are Bridged at AP and Bridged at AC. Select a VLAN from the list.

2. Select **Save**.

When a client connects to the network, a captive portal page is presented. The user enters a user name and password. The RADIUS authenticates the user name and password. Captive portal automatically generates two engine rules that define the Accept Policy for a client before authentication and after authentication.

Next, work with the ExtremeCloud IQ Controller engine rules.

Related Topics

Working with Internal Captive Portal Engine Rules on page 62

Working with Internal Captive Portal Engine Rules

When configuring captive portal, the ExtremeCloud IQ Controller Rules Engine creates default rules for network policy. Use the default rules and modify the Accept Policy when necessary.

1. Go to **Onboard** > **Rules**.

   Two new engine rules are displayed:

   - Unregistered LOC: Network: Test1- ICP (SSID of network)

     Prior to CP authentication, the client matches this rule and applies the **Accept Policy** of a non-authenticated role.
   - Web Authenticated LOC: Network: Test1- ICP (SSID of network)

     Once the client password is authenticated on the RADIUS server, the client matches this rule and applies the **Accept Policy** of the **Enterprise User** role.

     The **Enterprise User** is the default **Accept Policy**.

   Alternatively, you can create unique **Accept Policy** roles to be assigned upon authentication.

   a. Select the rule **Web Authenticated LOC: Network: Test1- ICP** and click ✎ to edit.
   b. From the **Accept Policy** field select a different value.
2. Click **Save**.

Next, modify the device group profile to enable the network and role options we are using.

Related Topics

Editing Device Group Profile for Network and Role on page 63

Editing Device Group Profile for Network and Role

Configure a network and be aware of policy roles that you are using before modifying the device group profile.

1. Go to **Configure** > **Sites** and select a site.
2. Click **Device Groups**.
3. Select **DeviceGroup_AP3915**.
4. Beside the Profile field, select ✎ to edit the default profile AP3915-default.
5. From the **Networks** tab, assign a radio to the network you created.
6. From the **Radios** tab verify that the radio that your network is assigned to is on and using the correct radio mode.
7. From the **Roles** tab, select the Accept Policy roles that the Rules Engine is using.

Note
Upon creating an internal captive portal network, the rules engine created two engine rules that make use of the following policies:

- Enterprise User
- Unregistered

External Captive Portal networks use the Unregistered policy by default, there is no user interaction.

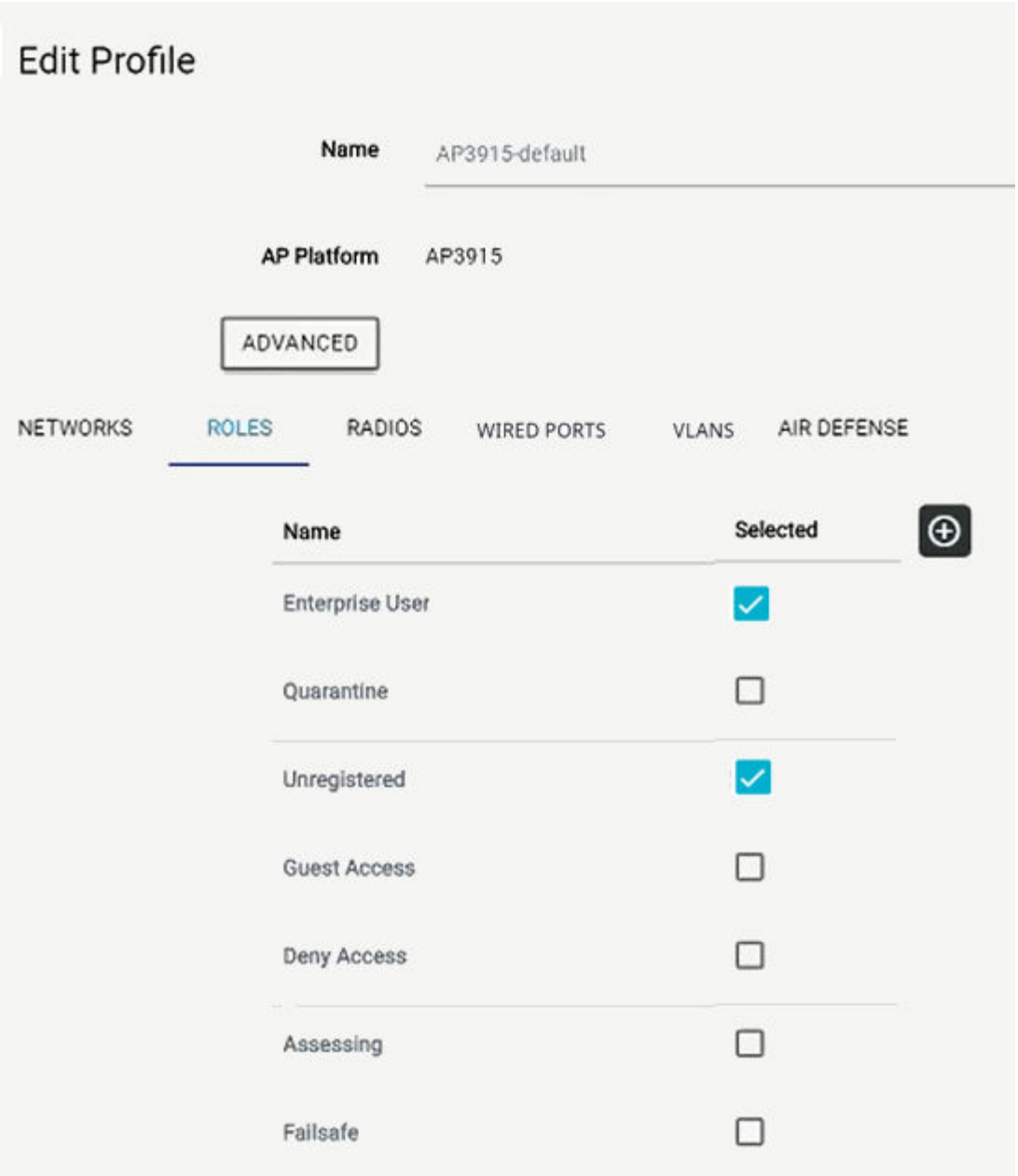


Figure 28: Edit Device Group Profile (Internal Captive Portal)

8. Optionally, you can configure settings from any of the available profile options. All APs in the device group are affected by options configured in the profile.

   Note
   The supported profile options depend on the AP Platform definition.

9. Click **Save** to save the profile settings.
10. Click **Close** to close **DeviceGroup_AP3915**

Currently, **Site_ROW** has **DeviceGroup_AP3915** with the following:

- 2 Roles

- 1 Network
- 1 Device

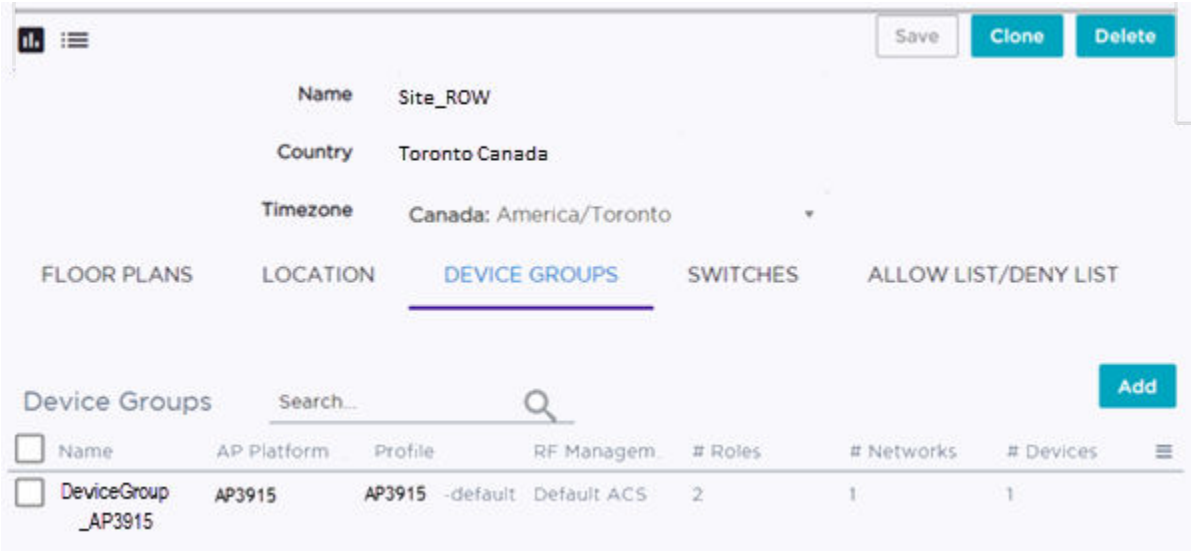


Figure 29: Centralized Site with Device Group

Next, configure adoption rules.

Related Topics

Creating Adoption Rules on page 65

Creating Adoption Rules

Configure a site and a device group before creating adoption rules. Adoption rules automatically assign devices to specific device groups upon registration with ExtremeCloud IQ Controller.

1. Go to **Configure** > **Adoption** > **Add**.
2. To create a rule for access points, select **AP**.
3. Select an Action.
4. Select a site and device group.
5. Specify a filter and select ⊕. The following are available parameters:

   IP Address/CIDR

   Filter the APs or switches by IP address, adopting APs into the specified device group based on their IP address. CIDR field is used along with IP address field to find the IP address range.

   For switch adoption rules, specify the management IP address.

   Host Name

   Filter the APs by host name, adopting APs into the specified device group based on their host name. This field matches on sub strings.

   For switch adoption rules, use the system name. The full host or system name is not required for a match.

Model

Model number on the device. This field matches on sub strings. The full model number is not required for a match.

Serial Number

Serial number on the device. Serial number requires an *exact* string match.

Note
Each filter value can only be applied once to a single rule.

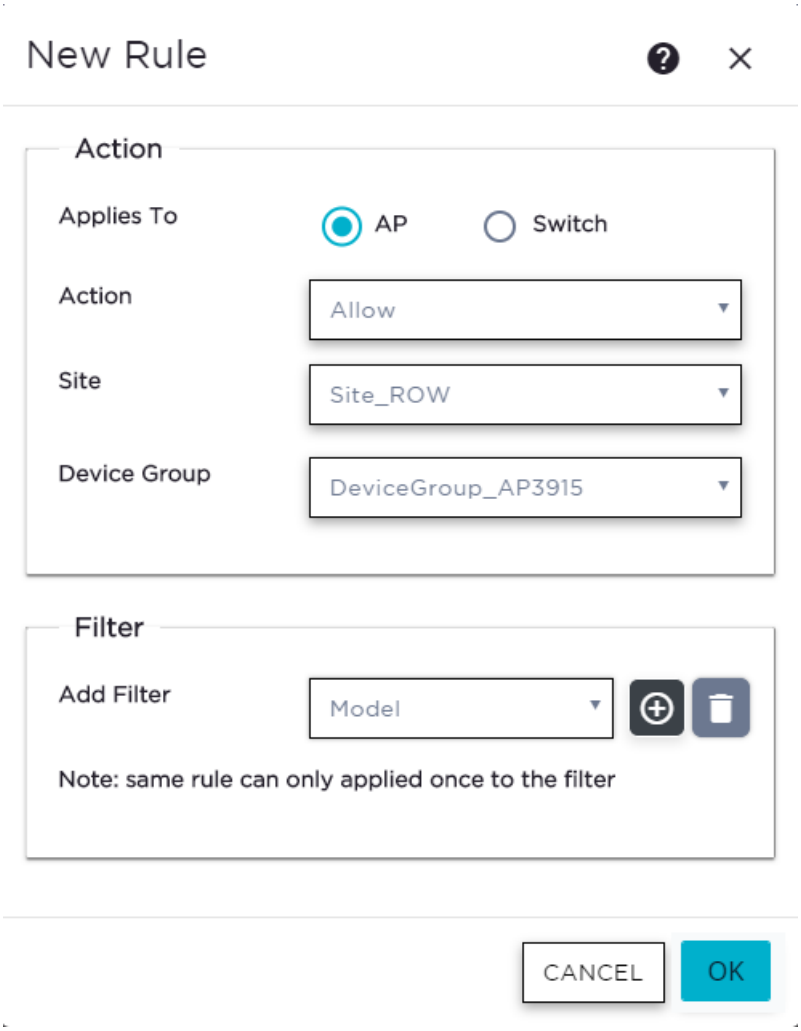


Figure 30: Create Adoption Rule

6. Select **OK**.
7. From the **Adoption Rules** page, select **Save**.

All AP3915 access points will be automatically added to **DeviceGroup_AP3915** within **Site_ROW** upon registration with ExtremeCloud IQ Controller.

Note

Be aware that all devices in a device group must share the following:

- AP model number
- Configuration Profile
- RF Management Profile

For more information on adoption rules, including Pattern-Based adoption and device redirection, see the *ExtremeCloud IQ Controller User Guide* located in the Extreme Networks documentation portal.

Centralized Site with a AAA Network

Configuring a AAA Network on page 68
Creating an Engine Rule on page 69
Creating a Policy Role on page 70
Applying a AAA Network and Role to the Device Group on page 71

Deployment Strategy

The following strategy outlines how to create a Centralized site with a AAA network.

1. Add a Centralized site with a device group.
2. Configure a AAA network.
3. Work with engine rules.
4. Create a policy role.
5. Specify the network and role in the device group profile.
6. Create adoption rules.

Configuring a AAA Network

Using the same Centralized site: **Site_ROW**, specify a separate tagged VLAN for the AAA Network, defining a different IP address range for the AAA Network.

Note
You can configure more than one network on a single VLAN, but to configure a separate IP address range for the AAA Network, we will create a separate VLAN.

1. Go to **Configure** > **Policy** > **VLAN** > **Add** to create a new VLAN for the AAA Network. For more information, see Specifying B@AC Network Topology on page 60.
2. Go to **Configure** > **Networks** > **Add** and configure the following parameters:

   Network Name

   Test2-AAA

   SSID

   Test2-AAA

   Status

   Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

   Auth Type

   WPA2 Enterprise 802.1x/EAP

AAA Policy

Local On-boarding

This option is not displayed for WLAN Networks that do not require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the ExtremeCloud IQ Controller. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal. AAA Policy can only be configured for WLAN Networks requiring MACAUTH, External Captive Portal, or EAP.

To use AAA Policy to bypass ExtremeCloud IQ Controller, create a policy with RADIUS servers and a NAS IP address, then specify the policy here. To get started, go to **Configure** > **AAA Policy** > **Add**. For more information, see the *ExtremeCloud IQ Controller User Guide* or *Online Help*.

Authentication Method

Default

Default AAA Authentication Method

Local

LDAP Configuration

None

Default Auth Role

Quarantine

Defines the default Accept Policy for a client attempting to join the network. When an authenticated client does not meet rule conditions on an 802.1x AAA Network, the default policy role is Quarantine.

Default VLAN

test2 (This is the VLAN we created for the AAA Network.)

3. Click **Save**.

Note
To activate the **Scheduling** button and schedule when network services are enabled, install the Extreme Scheduler Application on ExtremeCloud IQ Controller. For more information, see the *ExtremeCloud IQ Controller User Guide* located in the Extreme Networks documentation portal.

Next, work with engine rules.

Related Topics

Creating an Engine Rule on page 69

Creating an Engine Rule

Create a unique engine rule that applies the Enterprise User role upon authentication.

1. Go to **Onboard** > **Rules** > **Add** and configure the following parameters:

   Name

test2-rule

Rule Enabled

Select this box to enable the rule.

Location Group

Specify the Test2-AAA Network we created.

2. Select **Enterprise User** as the Accept Policy.
3. Click **Save**.

Next, create a unique policy role that this engine rule will apply upon authentication instead of **Enterprise User**.

Related Topics

Creating a Policy Role on page 70

Creating a Policy Role

You can create a policy role that will customize network access.

To create a new policy role:

1. Go to **Configure** > **Policy** > **Roles** > **Add** and configure the following parameters.

   Name

   myTest2-policy

   Default Action

   Set to **Deny**.

   The policy rule will deny everything except for the rules we define as allowed.
2. Select the **L3 L4 Rules** section and click **New**.
3. Configure the following rules:
   - Allow traffic to subnet 0.0.0.0/0, any protocol, Port DHCP Server (68).
   - Allow traffic to subnet 0.0.0.0/0, any protocol, port Port DHCP Client (67).
   - Allow traffic to subnet 10.48.51.50/28, any protocol, any port.
   - Allow traffic to subnet 10.48.49.9/32, any protocol, any port.
4. Click **Save** to save the policy.
5. Go to **Onboard** > **Rules**.
6. Edit the **test2-rule** Accept Policy. Apply **myTest2-policy** instead of **Enterprise User** policy.
   a. Highlight **test2-rule** and click ✎.
   b. From the Accept Policy field, select **myTest2-policy**.

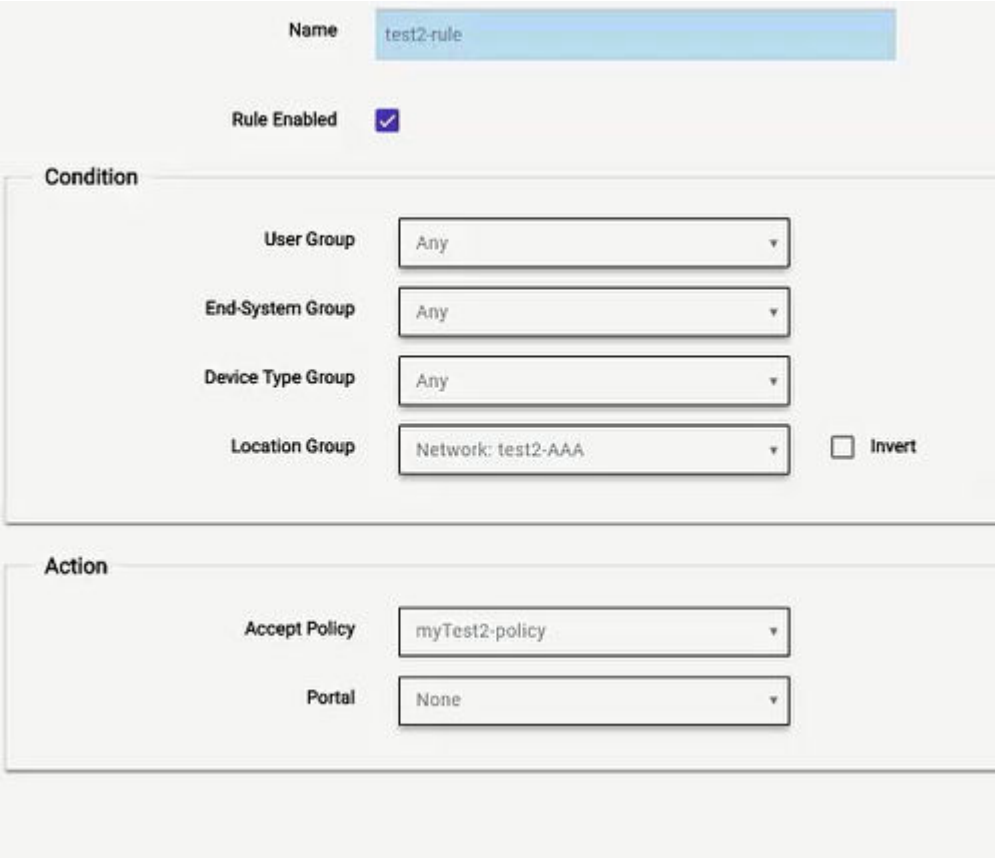


Figure 31: Engine Rule with Unique Policy

7. Click **Save**.

Upon authentication to the network, the client reaches the engine rule **test2-rule**. Client is accepted to the network based on the unique Accept Policy **myTest2-policy**.

Next, enable **myTest2-policy** within the device group profile.

Related Topics

Applying a AAA Network and Role to the Device Group on page 71

Applying a AAA Network and Role to the Device Group

Each time you configure a network or specify policy roles, you must enable the network and roles within the device group.

1. Go to **Configure** > **Sites** and select the site.
2. Select **Device Groups** tab.
3. Select **DeviceGroup_AP3915**.
4. Beside the Profiles field, select ✎ to edit the profile AP3915-default.
5. From the **Networks** tab, assign a radio to network **test2-AAA**.

   This is the AAA network we created.

6. From the **Roles** tab, select the Accept Policy roles we have configured under the Rules Engine. Quarantine is added to the list of roles.
   - Enterprise User
   - Quarantine
   - Unregistered
   - myTest2-policy
7. Click **Save** to save the profile settings.
8. Click **Close** to close **DeviceGroup_AP3915**.

Next, you have the option to create adoption rules for device group **DeviceGroup_AP3915**.

Related Topics

Creating Adoption Rules on page 65

Mesh Point Network Configuration

Mesh Point Network Settings on page 74
Configure Device Groups for Mesh Point on page 74
Advanced Configuration Profile and Mesh Device Settings on page 76
Configure Transparent Bridge on page 80

Deployment Strategy

The following strategy outlines how to configure a Mesh Point network:

1. Configure Mesh Point settings through the ExtremeCloud IQ Controller user interface.
2. Connect the Root AP to the backbone network using the AP GE1 port.
3. Connect the non-root APs to the backbone network using the AP GE1 port.
4. Wait for the non-root APs to receive the controller configuration.
5. Deploy the non-root APs.
6. If the wired network is bridged through the wireless mesh network, then connect the wired switch (or other device) to the non-root AP using the GE2 port.

Note

- Ports on the Universal APs are labeled with the prefix ETH.
- When a single interface AP is configured as a Mesh non-root AP, the single interface is used as a client port, not as an uplink.

Take the following steps to configure Mesh Point on the ExtremeCloud IQ Controller user interface:

1. Configure a Mesh Point Network. See Mesh Point Network Settings on page 74.
2. Configure Device Groups for Mesh Point on page 74.
3. From the device group configuration Profile:
   - Specify the Mesh Point Network.
   - Specify Advanced configuration Profile settings.
   - Specify Mesh Device Settings.

Initially, configure non-root APs over wired Ethernet, connected to the Management Port. After adding an AP to a non-root mesh device group, the AP will reboot and then it will be a member of the group without the Ethernet network. (It is highly

recommended to disconnect the Management Ethernet port at this time.) If you need to modify the configuration of a non-root AP after deploying in a mesh network, reconnect the AP through the Management Ethernet port and verify mesh point configuration. When a non-root AP is incorrectly configured in a mesh network, it can become stranded. To recover a stranded AP, reconnect to the Management Port through the wired Ethernet.

Related Topics

Mesh Point Network Settings on page 74
Configure Device Groups for Mesh Point on page 74
Advanced Configuration Profile and Mesh Device Settings on page 76

Mesh Point Network Settings

To configure a mesh point network, do the following:

1. Go to **Configure** > **Networks** > **Mesh Points** > **Add**.
2. Configure the following parameters:

   Mesh Point Name

   Name that identifies the mesh point.

   Mesh ID

   Identifies the mesh network. APs must have the same Mesh ID in order to form mesh links. APs with configured mesh points exchange beacons and the Mesh ID is checked. If a Mesh ID does not match that of the network, the beacon is dropped. If the Mesh ID does match that of the network, the AP adds an entry in the Mesh Point Neighbor Table.

   The SSID is used as the Mesh ID for networks that support AP39xx access points.

   Auth Type

   A pre-shared key (PSK) is used to AES encrypt traffic traveling between Mesh Point APs. Modifying the key after a non-root AP is deployed may cause it to become stranded. Connect the non-root AP through the Ethernet port before changing the PSK.

   Select **Edit Privacy** to enter the WPA2 key.

Configure Device Groups for Mesh Point

Configure AP Mesh Point settings from the AP configuration Profile, which is assigned at the device group level. The Root behavior setting for the AP is determined in the configuration Profile that is assigned to the device group, but this setting can be overridden from the AP Override settings for each AP. Differentiate the AP Root behavior setting one of two ways:

- **(Best Practice)** Configure two device groups: One device group for the root AP, one device group for the non-root APs. Configure separate Profiles with the appropriate Root behavior setting for each device group. For ease of configuration, you can copy configuration Profiles and make the necessary Root behavior changes.

- Configure one device group: From the configuration Profile, configure the Root behavior as non-root. Non-root is the correct configuration for all APs in the device group except for the one root AP. Then, override the Root behavior setting on that one root AP, configuring the designated AP as the root.

For this deployment example, we will configure two device groups: one for the Root AP and one for the non-root APs, creating two configuration Profiles.

Note
Mesh Point is supported on ExtremeWireless AP39xx, Wi-Fi 6 AP models. The mesh network must contain only AP39xx access points or only Wi-Fi 6 access points. You cannot combine the AP39xx platform with the Wi-Fi 6 access point platforms in a single mesh network.

To configure the device groups for Mesh Point:

1. Configure a site.

   Go to **Configure** > **Sites** > **Add** and configure the following site parameters:

   Name

   Site_ROW

   Country

   Select **Toronto Canada**.

   This value corresponds to the licensing domain ROW.

   Timezone

   Canada: America/Toronto
2. Create two device groups for the site. One for non-root APs, one for Root APs.

   All APs in a device group must share the following:

   - AP model number
   - Configuration Profile
   - RF Management Profile

   Go to **Configure** > **Sites** and select a site. Then, select **Device Groups** > **Add** and configure the following device group parameters:

   Name

   - Mesh_AP505_non-root
   - Mesh_AP505_root

   Profile

   AP505-default

   Select a configuration Profile that corresponds to the AP model. The configuration profile is specific to the AP model.
3. Select **OK**.
4. Select **Save** on the **Site** page to save the site and device group.
5. Repeat steps 2-4 to create a second device group for The Root access point.

The next step is to configure Advanced configuration Profile settings and Root behavior for the APs in the device group.

Related Topics

Advanced Configuration Profile and Mesh Device Settings on page 76

Advanced Configuration Profile and Mesh Device Settings

After you have configured a device group for the non-root APs and a device group for the root AP, configure the Profile settings:

- Verify configuration Profile **Advanced** settings.
- Configure Profile **Edit Mesh Device Settings**.

Profile Advanced Settings

Verify configuration Profile **Advanced** settings:

1. Go to **Configure** > **Sites** and select a site.
2. Select **Device Groups**.
3. Next to the **Profile** field, select .
4. Select **Advanced**.
   - A single mesh point is supported on multiple radios for a single AP. You can use different channels for each hop of a multiple hop mesh network. This can improve air time utilization and possibly increase throughput. However, multiple hops do not improve latency, so a best practice is to keep the number of hops less than two.
   - Radio settings for the root-AP and non-root APs must match.
   - When you add or remove a mesh point from a radio, the AP will reboot.
   - Dual-band support is available with Mesh Point. When one radio is configured for Mesh Point, both radios can provide service.
   - The recommended Poll Timeout setting for non-root APs is 60 seconds.
   - Transparent Bridge — To configure a Transparent Bridge, from the GE2 Port Function field select **Bridge**.

Edit Mesh Device Settings

Configure Profile **Edit Mesh Device Settings**. The **Edit Mesh Device Settings** depend on the device group AP model: Wi-Fi 6 or AP39xx.

> **Note**
> Configuration parameters you set from the configuration Profile **Mesh Points** tab apply to all APs in a device group. To override settings for a specific AP, see the AP Advanced Overrides. For more information, see the *ExtremeCloud IQ Controller User Guide*.

1. On the Profile **Mesh Points** tab, select a mesh network from the AP radio drop-down list.

   > **Note**
   > The access points are limited to one mesh point. Multiple radios can be configured for a single mesh point.

2. Select **Advanced**.

   The **Edit Mesh Device Settings** dialog opens.
3. Configure the following settings:

Table 9: Mesh Device Settings

AP Model	Option	AP Behavior
Wi-Fi 6 AP models	Root **Note:** Wi-Fi 6 access points can be part of the same mesh network, but they cannot participate in a mesh network with AP39xx. AP39xx access points must be a separate mesh network from the Wi-Fi 6 APs.	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. Select the root behavior of this mesh point. • **Yes** — Mesh point is root node for this mesh network. • **No** — Mesh point is not a root node for this mesh network. (Additional settings display.)
Wi-Fi 6 AP models	Monitor Primary Port Link	(Available for root APs) With Monitor Primary Port Link enabled, if a root AP loses connection to the backhaul, the non-root APs scan for a new root AP and the original root performs service as a non-root AP. When the original root AP restores connectivity, it resumes the role of root AP. Through the use of Automatic Channel Selection (ACS), the optimum path is restored.

Table 9: Mesh Device Settings (continued)

AP Model	Option	AP Behavior
Wi-Fi 6 AP models	Preferred Neighbor	(Available for non-root APs) Select the preferred Neighbor (AP name and radio) from a list of APs with a root or non-root mesh radio. When a non-root AP can see mesh beacons from more than one neighbor, this setting configures the AP to prefer one beacon over all others when choosing a path back to the root.
Wi-Fi 6 AP models	Preferred Root	(Available for non-root APs) Select the preferred root AP from a list of APs with a root mesh radio. Use this setting to balance the number of mesh points reporting to a specific root AP.
Radio Settings **Note:** Dual-band support is available with Mesh Point. When one radio is configured for Mesh Point, both radios can provide service.		Radio settings for the root-AP and non-root APs must match.
Wi-Fi 6 AP models	Channel Width	Represents the desired channel width. The channel width is set for all APs in a device group. Available options include: • Auto – Channel width is calculated automatically by the AP. It is displayed in the user interface for informational purposes only.
Wi-Fi 6 AP models	Channel Plan	Non-root APs are configured with Mesh ACS (Automatic Channel Selection). This allows the non-root AP to follow the channel and width of the uplink AP. The non-root AP scans channels to find the best path to a root AP. Preferred Root and Preferred Neighbor settings influence the path to the root AP. For APs that support 6 GHz, **PSC Channel** is an option. Because numerous channels are offered on the 6 GHz band, it is a best practice to configure the Preferred Scanning Channel (PSC) so that the amount of probing is kept to a minimum. Preferred channels function as primary channels at each channel width: 20, 40, 80, and 160 MHz. **Note:** Upon upgrade from earlier revisions, non-root APs in a mesh network are converted to Mesh ACS to determine the best channel.

Table 9: Mesh Device Settings (continued)

AP Model	Option	AP Behavior
Note: Path Minimum and Path Threshold are settings that refer to values in the Mesh Route Table. They are metric values determined by an algorithm that indicate when ACS scans for a better mesh point radio channel. The best route path algorithm includes elements such as hop count, data rates, RSSI, and loss rate. A perfect score is 1179.		
Wi-Fi 6 AP models	Path Minimum	The minimum root path metric value is used to evaluate the channel during the Mesh ACS scan process. Only the mesh point with a root path metric less than the minimum root path is considered a candidate mesh point that can hop to the mesh point root. Valid values are 100-20000. Default value is 1000. The lower metric value indicates a better quality mesh link to the root.
Wi-Fi 6 AP models	Path Threshold	The maximum root path metric value that determines when to evaluate the mesh point radio channel for a better path to the gateway. When the current path metric value exceeds this threshold, an ACS scan is triggered on the mesh point. Valid values are 800-65535. Default value is 1500. Setting this value below 1500 will result in more frequent channel scans.
Wi-Fi 6 AP models	Tolerance Period	This is a buffer period (in seconds) between when the metric value exceeds the Path Threshold and the scan begins. Set the number of seconds to allow the root path metric to recover before a scan begins. Valid values are 10-600. Default value is 60.
AP39xx	Root	• **Yes** - Mesh point is root node for this mesh network. • **No** - Mesh point is not a root node for this mesh network.

Table 9: Mesh Device Settings (continued)

AP Model	Option	AP Behavior
AP39xx Only	Path Selection Method	Select the method used for path selection in a mesh network. Available options include: • Uniform – The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths). Use this method for regular infrastructure meshing. • SNR-Leaf – Use this method in special infrastructure cases when it is more desirable to make path decisions based on SNR than on metric values.
AP39xx Only	Hysteresis Minimum Threshold	This is the minimum SNR value to consider a candidate for the next hop in a dynamic mesh network. For the AP39xx, this value maps to the Roaming Threshold value. • 100dB to 85dB maps to Low • 84dB to 70dB maps to Medium • 69dB to 0dB maps to High

Related Topics

Configure Device Groups for Mesh Point on page 74
Mesh Point Network Settings on page 74

Configure Transparent Bridge

A Transparent Bridge enables you to expand the wireless network by interconnecting the wireless APs through wireless links in addition to the traditional method of interconnecting APs via a wired network. A Transparent Bridge deployment is ideally suited for locations where installing Ethernet cabling is too expensive or physically impossible. Transparent Bridge:

- Enables connectivity over a mesh network without requiring policy enforcement.
- Carries VLAN tagged traffic between two areas of connection: trunk ingress-trunk egress.
- Typically used for point-to-point links.

To configure Transparent Bridge:

1. Configure a Mesh Point Network. See Mesh Point Network Settings on page 74.
2. Configure two device groups: One device group for the Root AP and one device group for non-root APs. See Configure Device Groups for Mesh Point on page 74.
3. From the non-root AP device group, configure the GE2 Port Function:
   a. Select **Advanced** to view Advanced Profile settings.
   b. From the GE2 Port Function field, select **Bridge**.

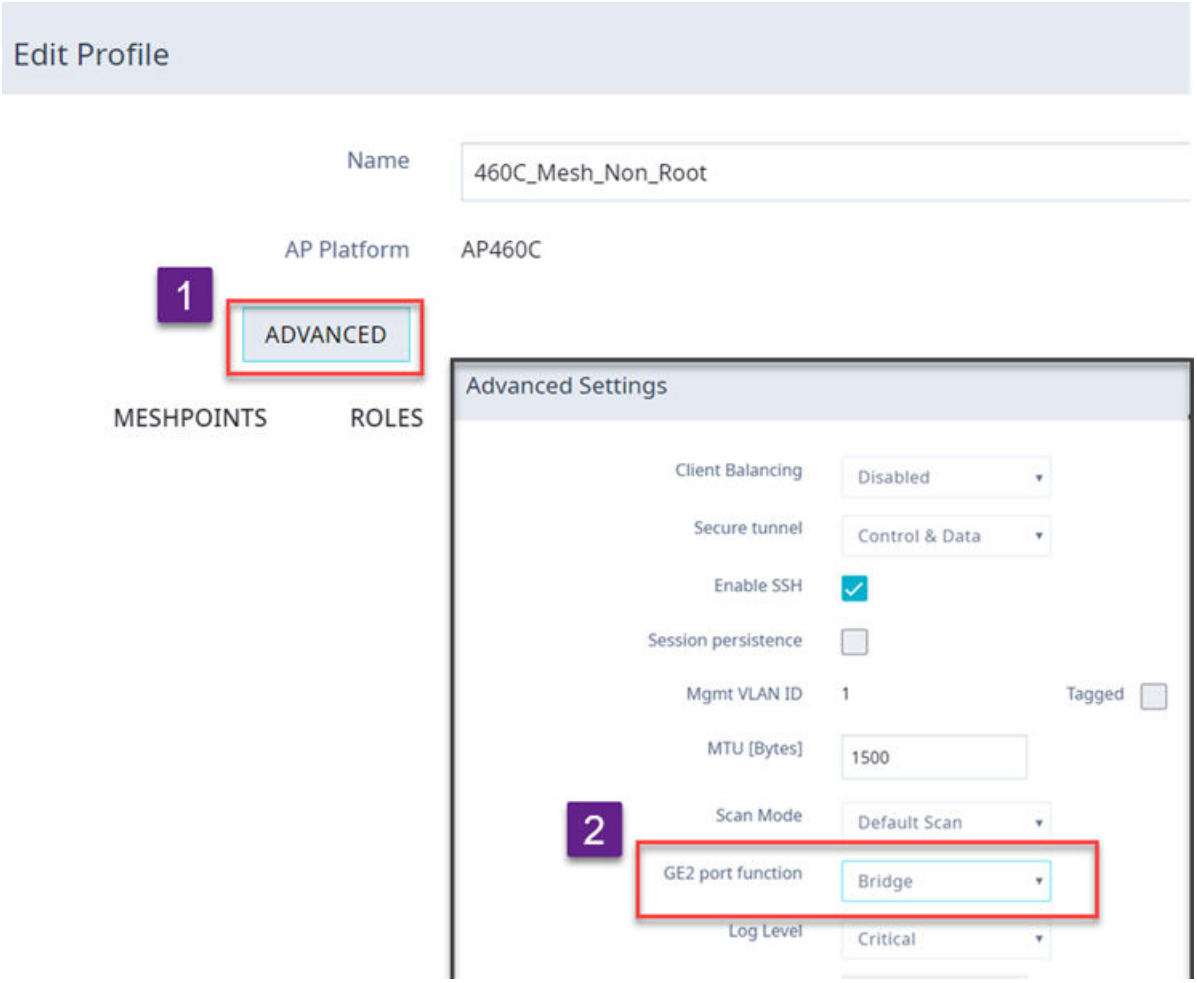


Figure 32: Configure Transparent Bridge from Device Group Configuration Profile

Note

Transparent Bridge provides a mesh link between two sites without requiring policy enforcement per device. Network policy and VLAN are not configured, and the **GE2 Port** field on the device group configuration Profile Networks tab is not displayed.

The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port.

You can configure Transparent Bridge for all APs in a device group and you can override settings for one or more individual APs from the AP **Advance Settings** > **Override** dialog.

Configuring an External NAC Server for MBA and AAA Authentication

Configuring the External NAC Server on page 83
Network with Default Auth Role on page 85
Network with Pass-Through External RADIUS on page 88

Deployment Strategy

The following deployment strategy uses an external NAC (Network Access Control) server to authenticate client sessions using MBA and AAA authentication methods. We will configure the “Use Default Auth” and the “Pass Through External RADIUS” Accept Policy actions upon successful user authentications.

For this strategy we are using the following:

- One of the following ExtremeWireless™ access points:
  - AP3000/X
  - AP302W
  - AP305C/CX
  - AP305C-1
  - AP310i/e
  - AP310i/e-1
  - AP360i/e
  - AP4000
  - AP4000-1
  - AP410i/e
  - AP410i-1
  - AP410C
  - AP410C-1
  - AP460i/e
  - AP460C/S6C/S12C
  - AP5010
  - AP5050U/AP5050D
  - AP505i
  - AP510i/e

- AP510i-1
- AP560i/h
- AP3917i/e/k
- AP3916ic
- AP3915i/e
- AP3912i
- AP3935i/e
- AP3965i/e

- An external NAC server running version 21.9.10 and an ExtremeCloud IQ - Site Engine server to manage and configure the NAC server.

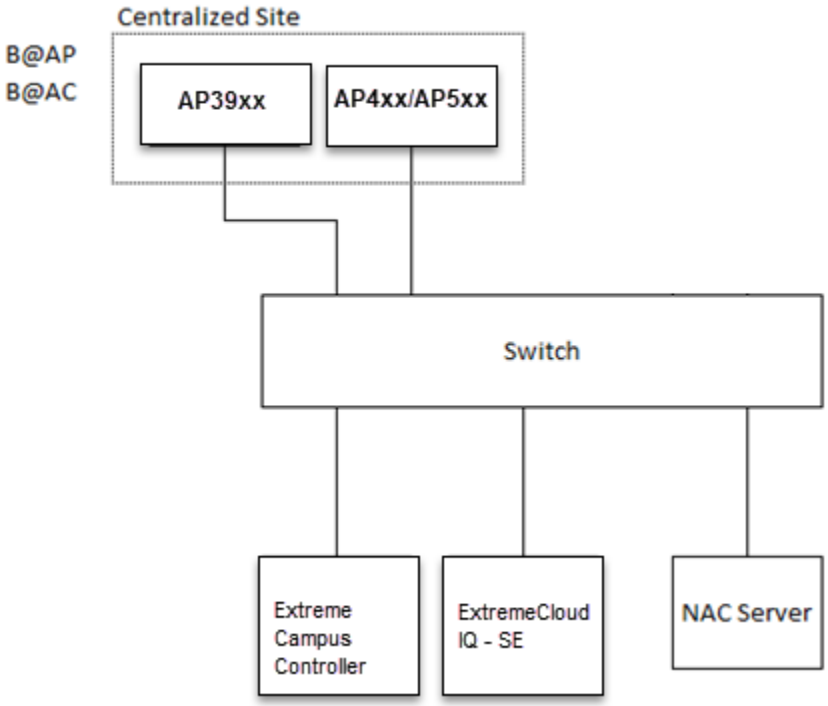


Figure 33: External NAC Server / ExtremeCloud IQ Controller Setup

Configuring the External NAC Server

Take the following steps to configure the External NAC server:

Extreme Management Center Console

1. Navigate to ExtremeCloud IQ - Site Engine OneView page or launch the console.
2. Add the external NAC server and the ExtremeCloud IQ Controller esa0 interface as devices to be managed by ExtremeCloud IQ - Site Engine.
   - Open NAC Manager using either OneView or the console.
   - Add the external NAC server as an appliance to be managed.
     a. Go to **Switches** > **Add Switch**.
     b. Select the ExtremeCloud IQ Controller esa0 interface

c. Configure the following parameters:

Primary Engine

NAC server

RADIUS Attributes to Send

Edit RADIUS Attribute Settings

3. To edit the RADIUS Attribute settings:
   - Select **Add** and provide the Attribute Group name.
   - In the Attribute field, enter the following:
     - Filter-Id=%FILTER_NAME%
     - Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME%
     - Login-LAT-Port=%LOGIN_LAT_PORT%
     - Service-Type=%MGMT_SERV_TYPE%

Note
The Attribute Group is configured to ensure that ExtremeWireless APs function with the appliance.

4. Save the Attribute Group, then select this group as the option in the **RADIUS Attributes to Send** field.
5. Press **OK**.

NAC Manager

6. Go to **Tools** > **Management**
7. Select **Configuration** > **Advanced NAC Configurations** > **AAA Configurations** > **Local Password Repository** > **Default**.
8. Add a new user.

   Select **Add** and configure the following parameters:
   - Display Name
   - Username
   - Password
9. Select **Save**.
10. In the **Advanced Configuration** window, navigate to **NAC Configurations** > **Rule Components** > **End-System Group**.
11. Add a new **End-System Group**.

    Add a new MAC entry for each MAC address of each client that should be successfully authenticated.
12. Select **Save**.
13. In the **Advanced Configuration** window, navigate to **NAC Configurations** > **Default**.
14. Add a new rule.

    From the End-System Group drop-down list, select the End-System Group that you previously created.

15. In the **Profile** drop-down list, select **Default NAC Profile**.

    Note
    Assuming no prior configuration changes have been made to the Default NAC Profile, it will send an *Enterprise User* Filter-ID.

16. Save the rule and move it up the list, just after the **Assessment Warning** rule.
17. Close the **Advanced Configuration** window and Enforce the NAC engine.
18. Once the Enforce is successful, close the window.

Network with Default Auth Role

The following procedure outlines how to configure a network and associate it with a Default Auth Role accept policy. The following network types are described:

- MBA Network
- AAA Network

Related Topics

Configuring an MBA Network on page 85
Configuring a AAA Network on page 86

Configuring an MBA Network

To create the MBA network associated to a Default Auth Role accept policy. Take the following steps:

1. Configure a RADIUS server for AAA authentication.
   - Log in to ExtremeCloud IQ Controller and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
   - Configure the following parameters:

     Radius Server IP Address
     Add the NAC IP address

     Shared Secret
     Provide the NAC Shared Secret.

     Note
     To find the Shared Secret of the NAC Manager, go to:
     Advanced NAC Configuration Settings > **Global and Appliance Settings** > **Appliance Settings**.

2. Create a new network.
   - Enable **MAC-based authentication (MBA)** and choose an appropriate MBA Timeout Role.
   - Clear the **Authenticate Locally for MAC** check box.
   - Choose **RADIUS** as the Authentication Method and select the NAC added in Step 1 as the Primary RADIUS.

- Select a Default VLAN.
- Click **Save**.

3. Add a new rule.
   - From ExtremeCloud IQ Controller, navigate to **Onboard** > **Rules**.
   - Click **Add**.
   - In the Location Group drop-down menu, select **Network: <name of your network>**.
   - From the Accept Policy field:
     - To configure a Default Auth Role Policy: select **Use Default Auth Role**.
     - To configure a Pass-thru External RADIUS Accept Policy: select **Pass Through External RADIUS**.
   - Save the rule.
4. Assign the network created previously and its Default Auth Role to a site and save. Take the following steps:
   - Go to **Configure** > **Sites** and select a site.
   - Click the **Device Groups** tab and select a device group.
   - Beside the Profile field, click ✎ to edit the device group profile.
   - Go to the **Networks** tab and select the configured network.
   - Go to the **Roles** tab and select the configured Default Auth Role.

Finally, associate clients to the SSID of the network. The Access-Request is sent to the external NAC server. The NAC server matches the MAC address of the user with one of the MAC addresses in the End-System Group (that was created earlier) and sends an Access-Accept with a Filter-ID *Enterprise User*. The ExtremeCloud IQ Controller Access Control engine ignores the Filter-ID and applies the Default Auth Role that was configured under Network Settings.

Configuring a AAA Network

To configure a AAA Network associated to a Default Auth Role accept policy. Take the following steps:

On ExtremeCloud IQ Controller:

Use the IP address of the external NAC server as the primary RADIUS server.

1. Configure a RADIUS server for AAA authentication.
   - Log in to ExtremeCloud IQ Controller and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
   - Configure the following parameters:

     Radius Server IP Address

     Add the NAC IP address

     Shared Secret

Provide the NAC Shared Secret.

> **Note**
> To find the Shared Secret of the NAC Manager, go to:
> **Advanced NAC Configuration Settings** > **Global and Appliance Settings** > **Appliance Settings**.

2. Create a new network.
   Configure the following parameters:

   Auth Type
   WPA2 Enterprise w/ RADIUS

   Authentication Method
   RADIUS

   Primary RADIUS
   IP Address of the External NAC added in Step 1.

   Default Auth Role
   Select a role other than *Enterprise User*.

   Default VLAN
   Select a Default VLAN. B@AP *VLAN ID*

   > **Note**
   > Both B@AP and B@AC are supported for NAC.

3. Select **Save**.
4. Create a policy rule.
   Go to **Onboard** > **Rules** and configure the following parameters:

   Location Group
   Network: *<name of your network>*

   Accept Policy
   - To configure a Default Auth Role Policy, select **Use Default Auth Role**.
   - To configure a Pass-Through External RADIUS Accept Policy, select **Pass Through External RADIUS**.
5. Select **Save**.

On the NAC Manager:

6. Edit the rule you created on ExtremeCloud IQ Controller here.
   Configure the following parameters:

   Authentication Method
   802.1x

   End-System Group
   Any
7. Select **Save** and enforce the NAC.

On ExtremeCloud IQ Controller:

8. Assign the network created previously and its Default Auth Role to a site and save.
   - Go to **Configure** > **Sites** and select a site.
   - Select the **Device Groups** tab and select a device group.
   - Beside the Profile field, select ✎ to edit the device group profile.
   - Go to the **Networks** tab and select the configured network.
   - Go to the **Roles** tab and select the configured Default Auth Role.

Associate clients to the SSID of the Network, when prompted for the username and password, use the username and password created with the New User. The external NAC server matches the rule you created under New Rule and upon successful authentication sends an Access-Accept and a Filter-ID *Enterprise User*. The ExtremeCloud IQ Controller Access Control engine ignores the Filter-ID and applies the Default Auth Role that was configured under Network Settings.

Network with Pass-Through External RADIUS

The following procedure outlines how to configure a network and associate it with a Pass-Through External RADIUS accept policy. The following network types are described:

- MBA Network
- AAA Network

Related Topics

Configuring an MBA Network on page 88
Configuring a AAA Network on page 89

Configuring an MBA Network

To create the MBA network associated to a Pass-thru External RADIUS accept policy. Take the following steps:

1. Configure a RADIUS server for AAA authentication.
   - Log in to ExtremeCloud IQ Controller and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
   - Configure the following parameters:

     Radius Server IP Address

     Add the NAC IP address

     Shared Secret

     Provide the NAC Shared Secret.

     Note
     To find the Shared Secret of the NAC Manager, go to:
     Advanced NAC Configuration Settings > **Global and Appliance Settings** > **Appliance Settings**.

2. Create a new network.
   - Enable **MAC-based authentication (MBA)** and choose an appropriate MBA Timeout Role.
   - Clear the **Authenticate Locally for MAC** check box.
   - Choose **RADIUS** as the Authentication Method and select the NAC added in Step 1 as the Primary RADIUS.
   - Select a Default VLAN.
   - Click **Save**.
3. Add a new rule.
   - From ExtremeCloud IQ Controller, navigate to **Onboard** > **Rules**.
   - Click **Add**.
   - In the Location Group drop-down menu, select **Network: <name of your network>**.
   - From the Accept Policy field:
     - To configure a Default Auth Role Policy: select **Use Default Auth Role**.
     - To configure a Pass-thru External RADIUS Accept Policy: select **Pass Through External RADIUS**.
   - Save the rule.
4. Assign the network created previously and its Default Auth Role to a site and save. Take the following steps:
   - Go to **Configure** > **Sites** and select a site.
   - Click the **Device Groups** tab and select a device group.
   - Beside the Profile field, click ✎ to edit the device group profile.
   - Go to the **Networks** tab and select the configured network.
   - Go to the **Roles** tab and select the configured Default Auth Role.

Finally, associate clients to the SSID of the network. The Access-Request is sent to the external NAC server. The NAC server matches the MAC address of the user with one of the MAC addresses in the End-System Group (that was created earlier) and sends an Access-Accept with a Filter-ID *Enterprise User*. The ExtremeCloud IQ Controller applies the *Enterprise User* Role instead of the Default Auth Role that was configured under Network Settings.

Note
The *Enterprise User* role must exist on ExtremeCloud IQ Controller and must be assigned to the same device group as the client in order to be applied.

Configuring a AAA Network

To create a AAA network associated to a Pass-thru External RADIUS Accept Policy. Take the following steps:

On ExtremeCloud IQ Controller:

Use the IP address of the external NAC server as the primary RADIUS server.

1. Configure a RADIUS server for AAA authentication.
   - Log in to ExtremeCloud IQ Controller and go to **Onboard** > **AAA** > **Radius Server** and add a new RADIUS server.
   - Configure the following parameters:

     Radius Server IP Address

     Add the NAC IP address

     Shared Secret

     Provide the NAC Shared Secret.

     Note
     To find the Shared Secret of the NAC Manager, go to:
     Advanced NAC Configuration Settings > **Global and Appliance Settings** > **Appliance Settings**.

2. Create a new network.

   Configure the following parameters:

   Auth Type

   WPA2 Enterprise w/ RADIUS

   Authentication Method

   RADIUS

   Primary RADIUS

   IP Address of the External NAC added in Step 1.

   Default Auth Role

   Select a role other than *Enterprise User*.

   Default VLAN

   Select a Default VLAN. B@AP *VLAN ID*

   Note
   Both B@AP and B@AC are supported for NAC.

3. Select **Save**.
4. Create a policy rule.

   Go to **Onboard** > **Rules** and configure the following parameters:

   Location Group

   Network: *<name of your network>*

   Accept Policy

   - To configure a Default Auth Role Policy, select **Use Default Auth Role**.
   - To configure a Pass-Through External RADIUS Accept Policy, select **Pass Through External RADIUS**.
5. Select **Save**.

On the NAC Manager:

6. Edit the rule you created on ExtremeCloud IQ Controller here.

   Configure the following parameters:

   Authentication Method

   802.1x

   End-System Group

   Any

7. Select **Save** and enforce the NAC.

On ExtremeCloud IQ Controller:

8. Assign the network created previously and its Default Auth Role to a site and save.
   - Go to **Configure** > **Sites** and select a site.
   - Select the **Device Groups** tab and select a device group.
   - Beside the Profile field, select ✎ to edit the device group profile.
   - Go to the **Networks** tab and select the configured network.
   - Go to the **Roles** tab and select the configured Default Auth Role.

Associate clients to the SSID of the Network, when prompted for the username and password, use the username and password created with the New User. The external NAC server matches the rule you created under New Rule and upon successful authentication sends an Access-Accept and a Filter-ID *Enterprise User*. The ExtremeCloud IQ Controller Access Control engine applies the *Enterprise User* Role instead of the Default Auth Role that was configured under Network Settings.

Note

The *Enterprise User* role must exist on ExtremeCloud IQ Controller and must be assigned to the same device group as the client in order to be applied.

Manage RADIUS Servers for User Authentication

RADIUS Settings on page 93
Advanced RADIUS Settings on page 93
Configure a Pass Through Rule on page 95

Configure a list of RADIUS servers to authenticate users of ExtremeCloud IQ Controller.

1. Go to **Administration** > **Accounts** > **RADIUS**.
2. To add a RADIUS server to the Authentication Order, under **Authentication Order**, select **Add**.

   Order the servers as Local first and RADIUS second until you have tested the RADIUS server.
3. To add the properties of the RADIUS server, under **RADIUS Servers**, select **Add**.

   Select the **IP Address** field to display a list of available RADIUS servers. Select the RADIUS server row to add or delete a RADIUS server.

   Note
   CHAP is the default authentication method used by ExtremeCloud IQ Controller. When configuring integration with ExtremeControl™ specify CHAP on ExtremeControl.

4. Select the **Test** button to test your server connection.

   Make sure the test completes successfully.
5. With the server order still Local first and RADIUS second, log in with your Active Directory user name and password.

   If this fails, make sure your Remote Access Policy is returning the required Service-Type of *Administrative*.

   Note
   To allow ExtremeCloud IQ Controller to accept the RADIUS Attributes coming from the External authentication server, configure a Pass Through External RADIUS Rule. Go to **OnBoard** > **Rules**.

Related Topics

RADIUS Settings on page 93
Advanced RADIUS Settings on page 93

Configure a Pass Through Rule on page 95

RADIUS Settings

Configure the following parameters and select **Save**.

Table 10: RADIUS Server Settings

Field	Description
RADIUS Server IP address	IP address of the RADIUS server.
Response Window	Determines the window of time, in seconds, that ExtremeCloud IQ Controller will wait for a response from the RADIUS server.
Authentication Timeout Duration	Determines a timeout value, in seconds, for the RADIUS server connection.
Authentication Retry Count	Determines the number of times ExtremeCloud IQ Controller will attempt to authenticate an end user.
Authentication Client UDP Port	User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic.
Proxy RADIUS Accounting Requests	Indicates that the RADIUS server will also handle RADIUS accounting requests.
Accounting Client UDP Port	UDP port number used for client accounting. User Datagram Protocol (UDP) needs only one port for full-duplex, bidirectional traffic.
Shared Secret	The password that is used to validate the connection between the client and the RADIUS server.
Mask	Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Related Topics

Advanced RADIUS Settings on page 93
Manage RADIUS Servers for User Authentication on page 92

Advanced RADIUS Settings

For information about advanced RADIUS configuration settings, see the following table:

Table 11: RADIUS Server Advanced Settings

Field	Description
Username Format	Determines if the domain name will be included in the username when proxying a request to the backend RADIUS server. Valid values are: • Strip Domain Name (default) - Select this option unless the backend RADIUS server requires the domain name to be included. • Keep Domain Name - Using this option with a Microsoft IAS or NPS server, may cause the server to timeout. Therefore, use an advanced AAA configuration. With a AAA configuration, only requests for known domains are sent to the backend RADIUS server. Unknown domains are processed locally and rejected.
Require Message-Authenticator	Protect against spoofed Access-Request messages and RADIUS message tampering with this attribute. The Require Message-Authenticator provides additional security when using PAP and CHAP security protocols for authentication. EAP uses the Message Authenticator attribute by default.
Health - Use Server Status Request	Use Server-Status RADIUS packets, as defined by RFC 5997, to determine if the backend RADIUS server is running.
Health - Use Access Request	Use an access request message to determine if the RADIUS server is running. The request uses a username and password. This method looks for any response from the server. The username and password do not need to be valid. A negative response will work. However, the username/password fields are provided to prevent rejects from being logged in the backend RADIUS server.
Check Interval	Determines the wait time between checks to see if the RADIUS server is running. **Note:** This is only applicable if the Server-Status request or Access request methods are used.
Number of Answers to Alive	Determines the number of times the RADIUS server must respond before it is marked as alive. **Note:** This is only applicable if the Server-Status request or Access request methods are used.

Table 11: RADIUS Server Advanced Settings (continued)

Field	Description
Revive Interval	Determines the wait time before allowing requests to go to a backend RADIUS server, after it stops responding. **Note:** Use this option only when there is no other way to detect the health of the backend RADIUS server. If Server-Status requests option and Access request option are not supported by the RADIUS server, then use this option.
Require Message-Authenticator	When enabled, the message-authenticator attribute value pair is included in the packet from the RADIUS server.
Health — Use Server Status Request	Determines if the Server Status Request is used to determine RADIUS server health upon recovery after the server has gone down. This is RADIUS status code point 12 from RFC5997.
Health — Use Access Request	Determines if the Server Access Request is used to determine RADIUS server health upon recovery after the server has gone down. This is access request code point 1 from RFC2865 with the user name/ password set to `fakeuser/fakepasswd`.

Related Topics

RADIUS Settings on page 93
Manage RADIUS Servers for User Authentication on page 92

Configure a Pass Through Rule

To allow ExtremeCloud IQ Controller to accept the RADIUS Attributes coming from the External authentication server, configure a Pass Through External RADIUS Rule.

1. From ExtremeCloud IQ Controller, go to **Onboard** > **Rules**.
2. Select **Add**.
3. In the **Location Group** drop-down menu, select **Network: <name of your network>**.
4. From the Accept Policy field:
   - To configure a Default Auth Role Policy: select **Use Default Auth Role**.
   - To configure a Pass-thru External RADIUS Accept Policy: select **Pass Through External RADIUS**.
5. Save the rule.

Related Topics

Manage RADIUS Servers for User Authentication on page 92

External Captive Portal on a Third-Party Server

Firewall Friendly External Captive Portal Flow of Events on page 97
Configure the Firewall on page 99
Configure an External Captive Portal on page 99
Understand Processing Performed by the ECP on page 100
Approve the Client on page 111
Compose the Redirection Response Sending the Browser back to the Appliance on page 112

ExtremeCloud IQ Controller supports integration with an External Captive Portal (ECP) on a third-party server.

An ECP is a web server that hosts a site that allows users to authenticate to the network. When the web server is not hosted on ExtremeCloud IQ Controller, the captive portal is considered a third-party ECP. ExtremeCloud IQ Controller intercepts and redirects the user's HTTP messages to the ECP web server.

ECP authentication involves filtering traffic of unauthenticated clients. When the client sends HTTP traffic, its browser is redirected to a website where the client's user can authenticate. The website is referred to as an ECP because it is located outside ExtremeCloud IQ Controller (which also offers an 'internal' captive portal). The ECP authenticates the user in whatever way it sees fit, and then tells ExtremeCloud IQ Controller or the AP whether the user is authenticated and what policy to apply to the user's session.

All interactions with the ECP are initiated by the user. The enterprise allows staff and guests to egress through port 80 on the firewall to use the third-party ECP.

We will discuss how to configure and program the ECP to interact with ExtremeCloud IQ Controller. This includes details about the message sequence that occurs when a client authenticates through an ECP. The following authentication flows are supported:

- A simplified flow in which ExtremeCloud IQ Controller accepts instructions from the ECP relayed through the client web browser.
- A more complex flow in which ExtremeCloud IQ Controller invokes RADIUS authentication to confirm the apparent authentication status of the client.

Firewall Friendly External Captive Portal Flow of Events

Typically, the third-party server is on the other side of a firewall from ExtremeCloud IQ Controller. Integrating with a third-party server through a firewall is illustrated in Figure 34 on page 97. The main participants in the deployment scenario are:

- The client being authenticated ('user').
- The ExtremeCloud IQ Controller that manages the AP that the user is communicating through.
- The firewall between the user and ExtremeCloud IQ Controller on one side and the ECP on the other.
- The ECP that performs the actual authentication.

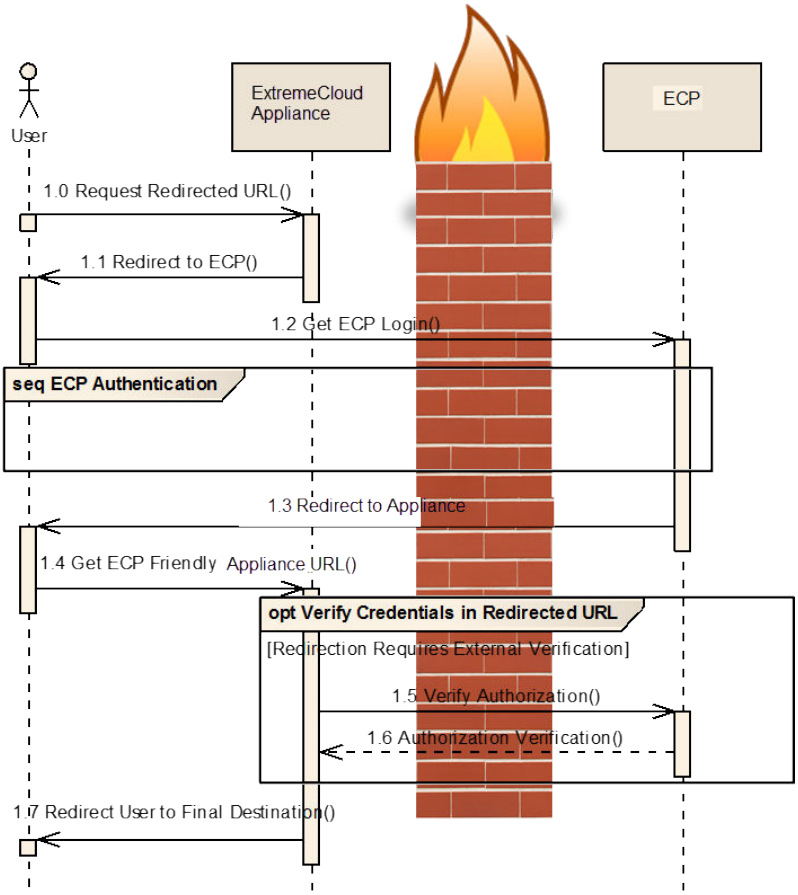


Figure 34: Firewall Friendly ECP Event Flow with ExtremeCloud IQ Controller

FF-ECP on ExtremeCloud IQ Controller

The following numbered list corresponds to the numbers illustrated in Figure 34 on page 97.

1.0 - When the user sends HTTP traffic, ExtremeCloud IQ Controller spoofs the destination web server.

1.1 - Traffic is redirected to the ECP. ExtremeCloud IQ Controller tells the client's browser that the resource it is requesting has temporarily been moved to another server (the ECP) .

ExtremeCloud IQ Controller adds parameters to the redirection, for example: the user's MAC address, the BSSID, or AP location, and AP Ethernet MAC. All available parameters are encoded into the URL request. The client's browser typically follows the redirection automatically. The redirection contains the query parameters added by ExtremeCloud IQ Controller.

1.2 - Because the ECP is located on a third-party server, the user's request must be forwarded through the enterprise firewall. Most companies allow requests for port 80 to pass through the firewall. Typically, the firewall also serves as a Network Address Translation (NAT). The NAT records the state of the connection, replaces the IP address in the request, and forwards it to the ECP.

When the ECP receives the redirected request, it typically replies with a web page. The client's browser sends subsequent requests to the ECP to retrieve additional content needed to render the page. If NAT is present, and the firewall allows it, the client establishes direct connection with the ECP web server, which serves the user experience and any necessary transactions related to the captive portal experience (including login, credentials collection, and validation).

ExtremeCloud IQ Controller is not involved in this interaction, except to forward traffic between the ECP and the client. The interaction can be as simple or complex as necessary (represented by the box labeled *seq ECP Authentication*).

1.3 - The ECP changes the client's authentication state and role. Once the server completes the captive portal workflow, the server responds to the client, instructing the client to redirect to ExtremeCloud IQ Controller. The status of the ECP authentication (and possibly credentials needed to have ExtremeCloud IQ Controller perform final authentication of the registering client) are encoded within the response message. You can display a set of terms and conditions on the ECP web page that the user must accept before a more liberal access control role is assigned.

1.4 - The client's browser usually follows the redirection URI automatically. Assuming the URI passes basic validation, the flow proceeds in one of two ways: If the URI contains a signature (secure hash) and the hash is verified by ExtremeCloud IQ Controller, the appliance accepts the user as authenticated. If the URI contains the name of an access control role defined on ExtremeCloud IQ Controller, it applies that role to all traffic that the client sends subsequently.

1.5 and **1.6** - If the URI is unsigned and contains a user name and password, then ExtremeCloud IQ Controller attempts to authenticate the user against a RADIUS server. The WLAN Service that redirects to the ECP must have at least one RADIUS server configured for authentication or an error is reported.

(Optional) If the ECP returns the credentials of the registered client (with the expectation that the appliance will perform final user authentication based on those parameters), the administrator can configure ExtremeCloud IQ Controller with the address and the shared secret of at least one RADIUS authentication server.

Instructions on how to configure a RADIUS server for a network using captive portal authentication is documented in the *ExtremeCloud IQ Controller User Guide* located in the Extreme Networks documentation portal.

The response from the RADIUS server may also contain attributes, such as maximum session duration, the VLAN to which the client's traffic is assigned, and the name of an access control role to apply to the traffic the client sends subsequently. If the attributes in the response are valid, ExtremeCloud IQ Controller applies them to the user session.

If no specific role is returned by the RADIUS server, then ExtremeCloud IQ Controller applies the Authorized role that is defined in the network configuration.

Once the user is authenticated, it is assigned to a new role that does not redirect its HTTP traffic to the ECP. The client's assigned role is enforced and access is granted or restricted based on the rules defined in the Policy role. Because this is a function of the role that the client gets assigned to, it is up to the ExtremeCloud IQ Controller administrator to define the authenticated role appropriately. The administrator can configure ExtremeCloud IQ Controller to steer the client back to the initially intended URL, or redirect the client to a specific URL.

1.7 - Assuming the client is authenticated, it has internet access to the extent allowed by the authenticated role to which it is assigned.

Configure the Firewall

Configure the firewall to enable clients that are behind the firewall to forward traffic to port 80 destination on the insecure side of the firewall. Most sites configure this behavior by default. A firewall friendly ECP can require the firewall to allow ExtremeCloud IQ Controller to forward RADIUS requests (UDP) to an external server (typically at port 1812).

Configure an External Captive Portal

The External Captive Portal (ECP) is, essentially, a web server that runs an application allowing clients to change their authentication state, by providing credentials, credit card details, demographic information about themselves or acknowledging terms and conditions. The application can be written in any language the ECP provider chooses. The ExtremeCloud IQ Controller web applications are implemented in PHP, but they will interact with any programming language or library on the ECP or client that can generate valid HTTP.

If the ECP expects the controller to sign redirection responses, it is critical that the real time clocks on ExtremeCloud IQ Controller and the ECP are synchronized. Signed redirection responses include timestamps to protect against replay attacks. Trust the redirection responses only for a limited period of time.

The easiest way to do this is to configure both ExtremeCloud IQ Controller and the ECP to use Network Time Protocol (NTP) to manage the clock. The time zone needs to be set correctly, both on the ECP and on the appliance. On ExtremeCloud IQ Controller, go to **Administration** > **System** > **Network Time** to configure NTP.

The timestamps in signed redirection responses are in UTC (Coordinated Universal Time). There is no need for ExtremeCloud IQ Controller to know the ECP's time zone and no need for the ECP to know the appliance's time zone.

The signing algorithm is a slight variation on Amazon Web Service's (AWS) algorithm for signing requests using query string parameters. At this time AWS makes an SDK available that includes implementations of the signing algorithms in several different languages (notably Java and PHP). It may be helpful to obtain and use this SDK rather than re-implement the signing algorithm from scratch.

Understand Processing Performed by the ECP

The ECP must receive HTTP/HTTPS redirection from ExtremeCloud IQ Controller, provide means for a client to become authorized, and finally redirect the user back to a web server on ExtremeCloud IQ Controller.

The script on the ECP that receives redirected requests has two responsibilities:

- Parse the redirection URL and preserve critical parameters for future use.
- Compose the web page that the user fills in to log into the network.

The Redirection URL Sent from ExtremeCloud IQ Controller

The request for the login page is in the form of an HTTP/HTTPS `GET` request. All the arguments to the request are passed as query strings appended to the URL. Typically, the web server or the back-end runtime system will parse the query strings and make them available to the back-end scripts.

The parameters that are described in Table 12 on page 101 are included in the URL statement sent from ExtremeCloud IQ Controller. The following parameters are required to be included in the return statement to ExtremeCloud IQ Controller:

- wlan
- token
- role
- user name
- password

Additional parameters are provided optionally for reporting purposes.

Table 12: Parameters Available on the Redirection URL from ExtremeCloud IQ Controller to the ECP

Parameter Name	Parameter Value	Required	Notes
ap		No	The AP Name to which the authenticating user has associated.
bssid	Alphanumeric String	No	The BSSID to which the authenticating client has associated. The BSSID is a MAC address belonging to the AP to which the client associated. The BSSID is in the format of six hex digits. The hex digits are “0123456789abcdef”. An example BSSID could be “00026fe9b568”. This is the same value that would be included in the Called-Station-ID field of a RADIUS Access-Request sent on behalf of this client.
ssid	A character string up to 32 bytes long	No	The SSID (Service Set Identifier) to which the client associated. ASCII-encoded hex string.
dest	Alphanumeric string	No	This is the original URL that the client’s browser was trying to receive when the request was redirected. The string is URI-encoded. For example, slashes in the URL are replaced by “%2F”.
hwc_ip	Numeric String	No	This is the IP address to which clients should be redirected to complete authentication. Typically, an appliance ends up with many IP addresses, but only one of them will map to the WLAN service’s ECP implementation. **Note:** This address may not be accessible directly by the ECP. However, it will be accessible to the client that is being authenticated. This attribute appears in the redirection response from the appliance. A sample hwc_ip address is “10.10.21.6”.
hwc_port	ASCII-encoded numeric string	No	This the port on the appliance interface to which the client should be redirected. If ECP support is configured for HTTP then the hwc_port will be “80”, otherwise it will be “443”. This attribute appears in the redirection response from the appliance.

Table 12: Parameters Available on the Redirection URL from ExtremeCloud IQ Controller to the ECP (continued)

Parameter Name	Parameter Value	Required	Notes
mac	ASCII-encoded hex string	No	The MAC address of the client that is being authenticated. A client could have multiple MAC addresses. This MAC address is the MAC address of the client's wireless interface that it used to associate to the wireless network. The client MAC address is in the format of six hex digits. The hex digits are "0123456789abcdef". An example "mac" could be "0023149032a8". This is the same value that would be included in the Calling-Station-ID field of a RADIUS Access-Request sent on behalf of this client.
role	Alphanumeric String	Yes	The name of the access control role to which the authenticating client is assigned at the moment of redirection. A best practice is to use the ExtremeCloud IQ Controller default roles.
sn	ASCII-encoded hex string	No	The serial number of the AP to which the client being authenticated associated. The serial number identifies the AP. It is assigned to the AP at manufacturing time. The serial number is a sequence of hex digits with the 'alphabetic' characters in lower case. "12b2694560000000" is an example of an AP serial number.
token	Alphanumeric String	Yes	An identifier for the user's wireless session hosted on the appliance that performed the redirection.
vlan	ASCII-encoded decimal number	No	The VLAN ID of the VLAN/topology to which the client is assigned at the moment of authentication. The VLAN ID is a number in the range 1 to 4094. The VLAN ID is the containment VLAN of the default action of the role to which the authenticating client is assigned. A role's default action does not have to be "contain to VLAN". If the default action is not "Contain to VLAN" then this attribute will be empty or not present.
vns	Alphanumeric String	No	The name of the Virtual Network Service (VNS) on which the client is authenticating. In ExtremeCloud IQ Controller, this value is treated as the `ssid-name`.

Table 12: Parameters Available on the Redirection URL from ExtremeCloud IQ Controller to the ECP (continued)

Parameter Name	Parameter Value	Required	Notes
wlan	ASCII-encoded decimal string	Yes	An internal identifier for the WLAN service on which the client is authenticating. The `wlan` attribute must be present in all redirection responses (and redirected requests) sent by the appliance. The ECP must return the wlan attribute in the redirection back to the appliance that it sends to the authenticating client's browser.
X-Amz-Algorithm	Alphanumeric String	No	The identifier for the algorithm used to compute the "X-Amz-Signature". Only present when the appliance is configured to sign the redirection. This attribute must be present when the appliance is configured to sign the redirection. The value of this attribute is "AWS4-HMAC-SHA256" and is not configurable. The signing algorithm and the role of the identifier in it are covered in more detail in section Verify the Signed Request on page 104.
X-Amz-Credential	Alphanumeric String	No	The identifier for the account whose shared secret was used to compute the "X-Amz-Signature". Only present when the appliance is configured to sign the redirection. If the appliance is configured to sign the redirection then this field must be present. This is covered in more detail in section Verify the Signed Request on page 104.
X-Amz-Date	Alphanumeric String	No	This is the time at which the appliance prepared and sent the redirection back to the user's browser. The date and time are in ASCII-encoded UTC. This attribute is present if a time stamp or a signature is requested. It can be used to identify stale or replayed URLs. If the appliance is configured to sign the request this must be included in the redirection response (and the browser's redirected request).

Table 12: Parameters Available on the Redirection URL from ExtremeCloud IQ Controller to the ECP (continued)

Parameter Name	Parameter Value	Required	Notes
X-Amz-Expires	Numeric String	No	This is the maximum length of time in seconds to trust the request. In other words the web request is only good until X-Amz-Date + X-Amz-Expires. After that time the URL should not be trusted as it is highly likely to have been replayed. This attribute is present only when the appliance is configured to sign the redirection to the ECP, in which case it must be present.
X-Amz-Signature	ASCII-encoded hex string	No	This is the signature computed over some of the HTTP headers and parts of the query string, presented as ASCII encoded-hex. The field is present only when the appliance is configured to sign the request.
X-Amz-SignedHeaders	Alphanumeric String	No	Which of the headers in the HTTP request were included in the input to the calculation of the signature. This is present only when the appliance is configured sign the redirection to the ECP, in which case it must be present.

Verify the Signed Request

When the controller is configured to include signatures, it is easy for the ECP to ignore them. The ECP simply extracts the information it is interested in from the provided attributes and ignores the rest.

However, it is highly likely that an administrator that enables response signing wants to use the signatures to authenticate the redirected requests it receives. This section covers how to do that. The whole process is shown in Verifying a Signed Request Basic Validation Checks on page 107.

The algorithm used to sign the redirection response (and therefore the redirected request to the ECP) is based on Amazon Web Services API Signature Version 4. AWS documentation refers to this approach as “Pre-signed URLs”.

Basic Steps

The following steps indicate the basic procedure for verifying the signature. Refer to Figure 35 on page 106 for the graphical flow.

1. Perform basic validation on the request message (are all required fields present, is the date current?). If these validations fail, there is no point in computing the signature.
2. Extract the signature from the received request.

3. From the received request, construct the string over which the signature will be computed. All but one component of this string come from the query parameters.
4. Generate the signing key. The shared secret is used to generate a signing key and is not itself the signing key.
5. Generate the signature using the signing key and the constructed string.
6. Compare the extracted signature (X-Amz-Signature) to the signature just computed. If they do not match, the request is invalid and should be discarded.

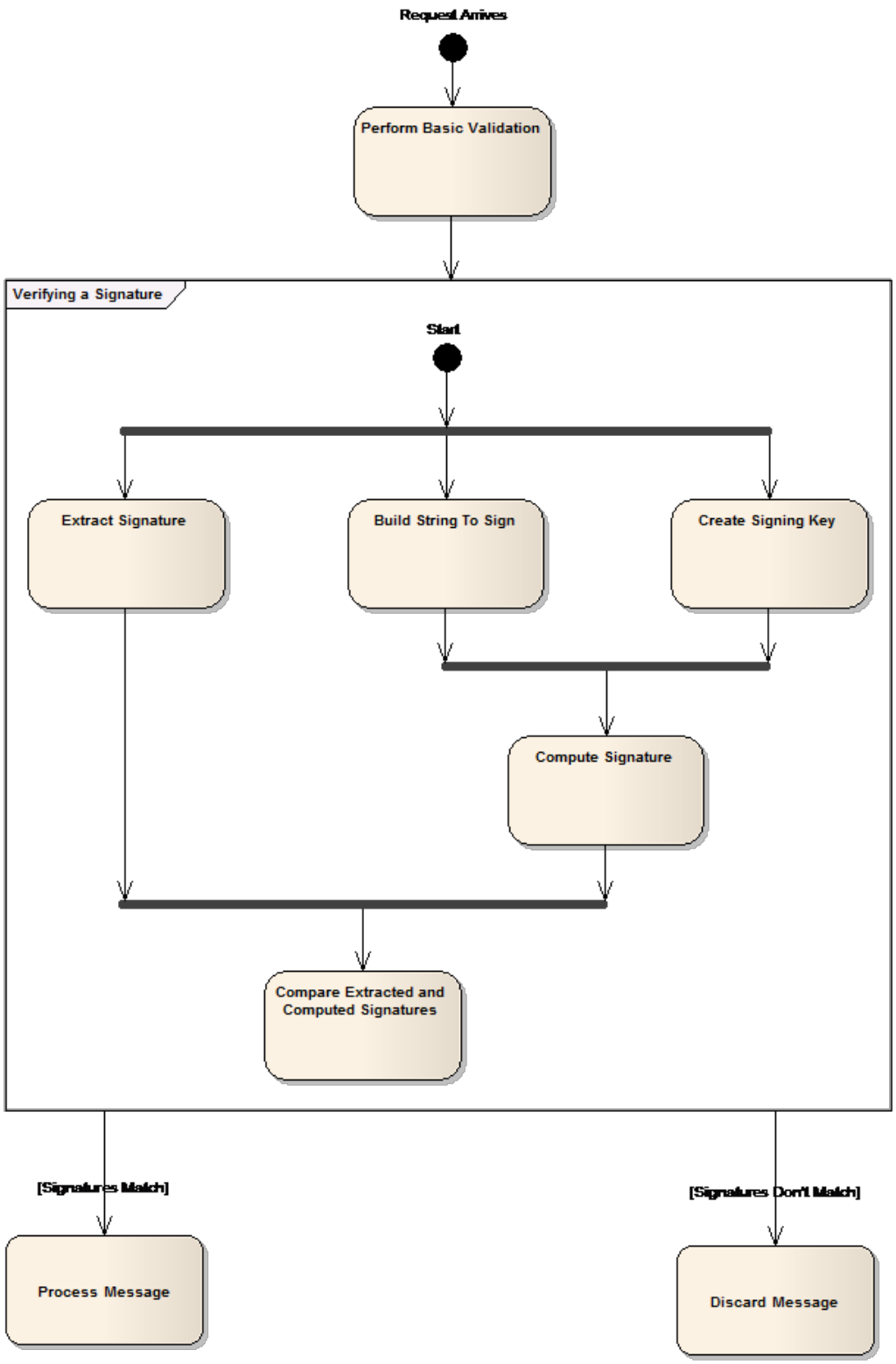


Figure 35: Basic Flow for Verifying a Signature

Verifying a Signed Request Basic Validation Checks

The following items can be considered when validating the redirect prior to computing the signature:

1. Does the request contain a token parameter, a WLAN parameter, and a destination URL? If not, the request either did not come from the controller or was tampered with en route.
2. If the request contains a timestamp, does the timestamp meet the following requirement:

```
timestamp <= now <= timestamp + x_amz_expires
```

Or if an allowance for clocks being out of sync is made,

```
timestamp - fuzz <= now <= timestamp + x_amz_expires
```

If not, the request is invalid, possibly the result of a user bookmarking the ECP landing page on a previous visit. The request should be rejected or discarded.

1. Are all parameters formatted in accordance with the descriptions?
2. Are all parameters required for the signature present in the request?

The first 1/3 of “verifyAwsUrlSignature” and the private method “validateQueryParms” in section crypt_aws_s4.php on page 229 provide examples of performing these types of checks in PHP.

Extracting the Signature from the Request

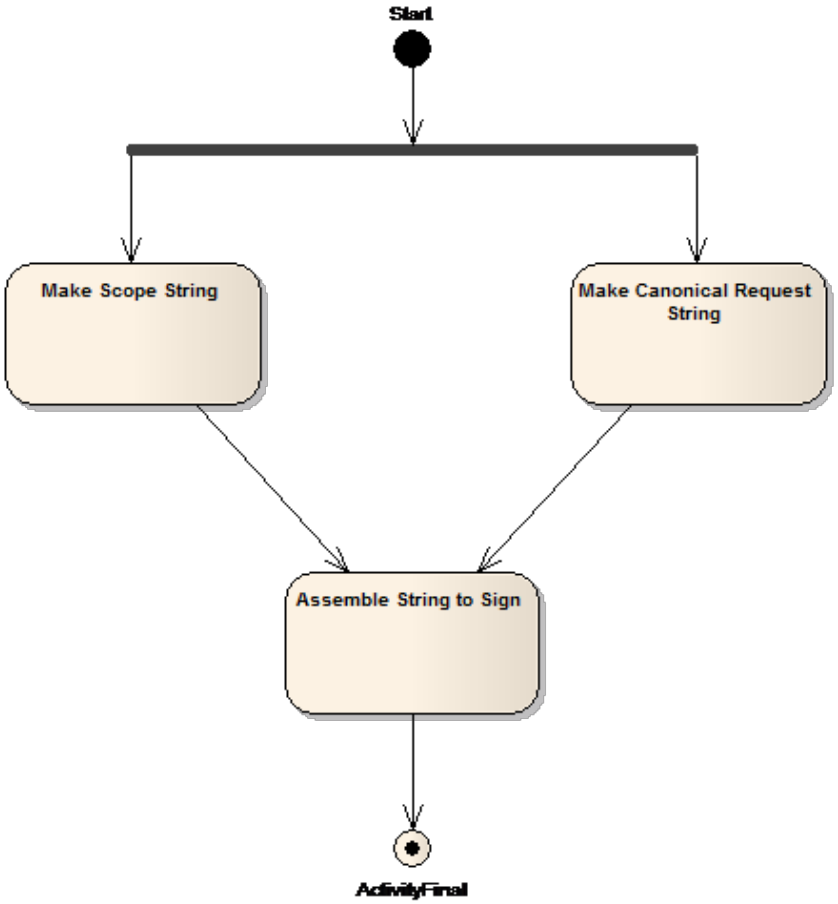
The signature is in the “X-Amz-Signature” query string parameter. Obviously the signature itself can’t be included in the computation of the signature so it must be removed from the request and set aside for later comparison. How the signature is removed from the request will depend on the program language and framework used to implement the external captive portal. The method “simpleaws::verifyAwsUrlSignature” in crypt_aws_s4.php on page 229 illustrates one way to remove the signature when the query parameters are in a PHP array.

Building the String to Sign

Figure 36 shows the main actions required to build the string that will be signed out of the request:

1. Build the scope string.
2. Build a “canonicalized” version of the request.
3. Assemble the scope string, the canonicalized string, and some additional inputs to create the string to sign.

The scope string is easy to build out of a valid request. It is made from parts of the string in the “X-Amz-Credentials” parameter. If the credentials are valid then the scope string can be created by un-escaping the forward slashes it contains (i.e. replace ‘%2f’ with ‘/’), and then taking all the characters to the right of the first forward slash. The scope ends up being the fully qualified credential, less the identity string.



Note

Parts of the Scope

The fully qualified Amazon credential consists of:

- An identity string (the one configured in the controller GUI).
- The date portion of the X-Amz-Date.
- A region string. For a real Amazon application this is one of the geographic service regions defined by Amazon. The service region is not critical for the FF-ECP implementation so it is always set to 'world'.
- A service identifier. The service is always set to 'ecp'.
- The identifier 'aws4_request', which identifies the signature version.

Figure 36: Steps in Building the String to Sign

The canonicalized request string has the format:

```
"GET\n"
.<URL-Path-Component>."\n"
.<URL-Query-Parameters>."\n"
.'host:'.<URL-Host>
."\n\nhost\nUNSIGNED-PAYLOAD";
```

Where:

- `GET` is the request type. For FF-ECP this will always be the literal "GET."
- `<URL-Path-Component>` is the substring beginning with the '/' at the end of the host or host-plus-port portion of the URL and either the end of the URL or the '?' marking the beginning of the query parameter string. For example, the URL-Path-Component of `https://192.168.18.152:5825/adir/bdir/cdir/resource.htm?x=7&y=gg` is `/adir/bdir/cdir/resource.htm`
- `<URL-Query-Parameters>` is the substring following the '?' character and extending either to the end of the URL or up to but not including the '#' fragment character.
- `<URL-Host>` is the host portion of the URL string. It excludes any port number included in the URL. In the preceding URL, the URL-Host is 192.168.18.152.
- '`.`' is the catenation operator.
- The remaining components are literals that should be added to the string as-is.

Finally the string that will actually be signed is composed as:

```
"AWS4-HMAC-SHA256\n"
.<Date>."\n"
.<scope>."\n"
.sha256(<canonicalized-request-string>)
```

where

- `AWS4-HMAC-SHA256` is a literal identifying the overall signing algorithm being used.
- `<Date>` is the value of the "X-Amz-Date" parameter extracted from the redirected request.
- `<Scope>` is the scope string that was assembled as described above.
- `<canonicalized-request-string>` is the canonicalized request string assembled as described above.
- `sha256()` is a procedure that applies the standard sha256 algorithm to the canonicalized-request-string. Its output should be in the form of a string of lowercase hex digit characters.

Creating the Signing Key

The process for generating signatures uses symmetric key encryption. The controller and the ECP use a shared key (the one configured on the controller's WLAN Service's captive portal configuration dialog) and the same encryption algorithm to generate and validate the signature.

The shared key is not used directly. Instead it is used to generate a secure hash ("HMAC") that is then used as the key to sign the request. The process for creating the key is shown below in Figure 37.

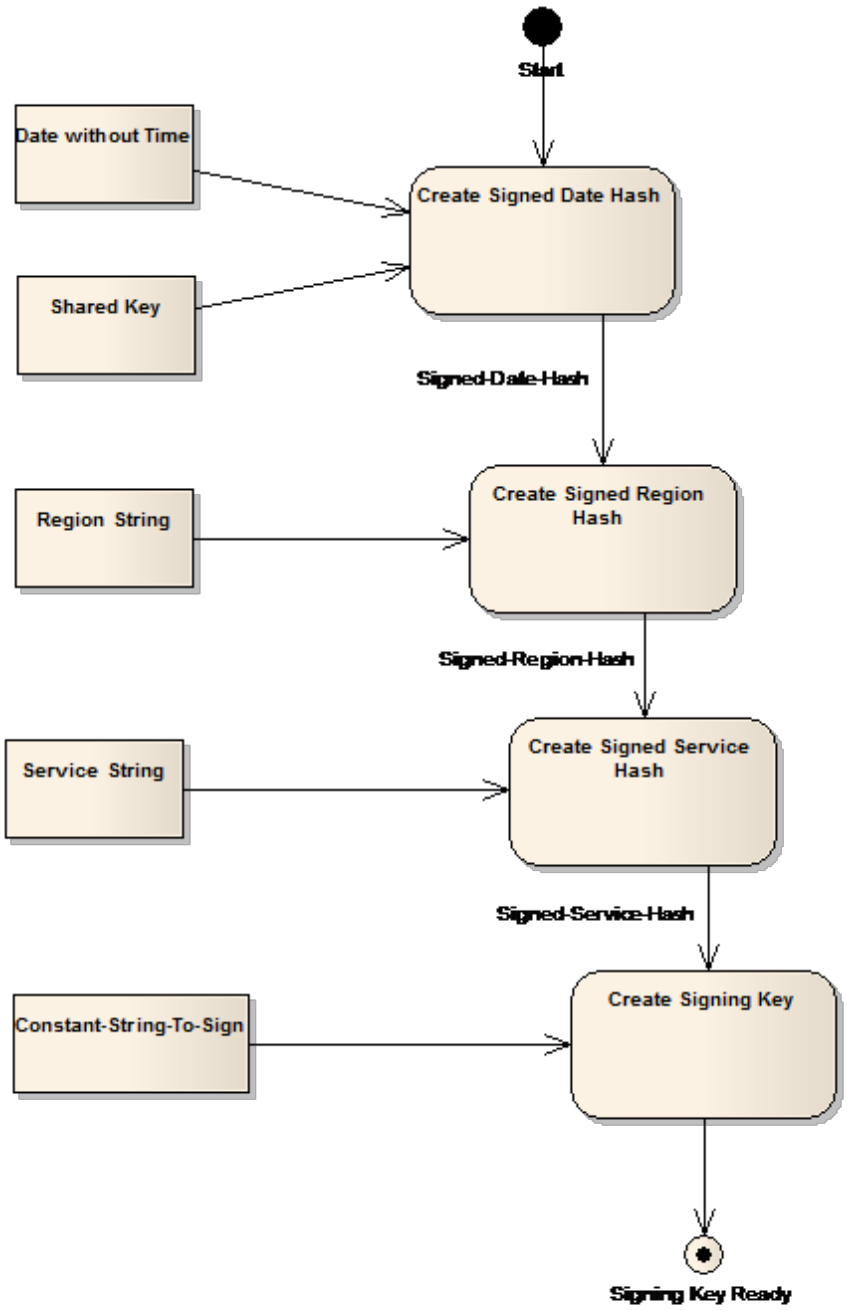


Figure 37: Creating the Signing Key

In the above figure:

1. “Date without Time” is the first 8 characters in the “X-Amz-Date” attribute, which corresponds to the date only in “YYYYMMDD” format.
2. “Shared Key” is the shared key configured on the controller. It is the shared key that is paired with the identity used to create the “X-Amz-Credential” attribute in the redirected request.

3. “Region String” is the region component of the Scope string.
4. “Service String” is the service component of the Scope string.
5. “Constant-String-To-Sign” is the string “aws4_request”.

And each of the “Create...” actions consists of generating a secure HMAC using SHA256 from the inputs. The output secure hash is in binary format (not encoded as a hex character string). The output of each step acts as the signing key for the subsequent step. The signing key for the first step is the shared secret, pre-pended with the literal ‘AWS4’.

Note that for any given identity the correct signing key only needs to be computed once per day. If the calculations are cached the cache should include an entry for the previous day to cope with the request being sent just before midnight UTC. The previous day’s key only needs to be kept for a small overlapping period (perhaps 10 minutes at the most).

Creating the Signature and Verifying the Request

At this point the signature for the request is computed as a secure HMAC using SHA256. The signing key is created as described in Creating the Signing Key and the string to sign is created as described in Building the String to Sign on page 107.

Verifying the signature in the request consists of standard string comparison between the transmitted and computed keys. If they aren’t identical the request is invalid. The client can be sent a web page containing a generic reject message or the request can be discarded silently.

Compose the Login or Splash Screen Page

How you create the login page depends on the programming language and toolset you use. This is largely outside the scope of this document. You can use any programming language that can be used for web development to create an external captive portal.

The content on the login page depends on the overall environment the ECP serves. It can contain as little as terms and conditions and a button to indicate acceptance, or it can contain fields necessary to submit a user ID and password.

The redirected request contains the attributes configured on the ECP configuration dialog. Attributes can be used to decorate the login page, and other information can be input to the authentication process. For example, a user may be considered authenticated only after logging in from one of a specific set of APs.

Approve the Client

Typically, users submit credentials for authentication into an ECP. The credentials are submitted in an HTTP “post”. The post invokes a script on the ECP web server passing the user’s credentials to the script as arguments. Write the script that is adapted to your specific requirements.

The script file can have any name. For this example, the script is named “login.php”. The script can be written in any programming language that supports web development. For this example, the script is written in PHP.

The main job of the “login.php” script is to co-ordinate the client’s browser, the back-end authentication server, and the appliance. The “login.php” script takes the submitted credentials, sends them to an authentication server, and waits for the server’s reply. The exact steps taken here depend on the selected programming language, operating system, and the type of authentication server selected.

After the authentication server has verified the user and potentially returned an access control role to assign to the user, the script needs to tell the appliance that the user is authenticated and indicate the role to assign to the user. The ECP informs the appliance by putting the information in the query string of a redirection response. The redirection response sends the client’s browser to a web server running on a specific interface and port of the appliance that hosts the client’s session. The client’s browser normally sends a redirected request immediately and automatically.

The redirection response does not need to be signed. If it is not signed, the appliance does not use the session attributes that are included in the redirected request. Instead, the appliance expects the redirected request to include a user ID and password. These credentials are sent to a RADIUS server in a standard RADIUS Access-Request. The redirected request is considered *invalid* if:

- The redirected request is not signed, and
  - The redirected request does not contain a user ID or password, or
  - The WLAN Service the client is using does not have at least one RADIUS server configured for authentication.

An invalid redirected request is sent to a standard error page. The error page cannot be configured at this time.

Compose the Redirection Response Sending the Browser back to the Appliance

Signing the Redirection to ExtremeCloud IQ Controller

Signing the redirection response is a similar process to calculating the expected signature for a URL that was received at the ECP. In fact, it is the same algorithm, but the inputs to the algorithm are not taken from the request as the request is under construction.

There are only two steps involved in signing the redirection response from the ECP:

1. Compose the pre-signed redirection URL to be signed.

   This step consists of building the request URL as described in Case 1: When a RADIUS Server Authenticates the Client on page 113 or Case 2: When the ECP is the Final Authority on page 115 but leaving off the `X-Amz-...` parameters that are required for the signature.

2. Sign the URL, adding all parameters to the URL that are required to sign it.

   This step consists of generating the signature, then appending all the `X-Amz-...` parameters used to the URL. This processing is described in Building the String to Sign on page 107, Creating the Signing Key on page 109, and Creating the Signature and Verifying the Request on page 111.

Related Topics

Case 1: When a RADIUS Server Authenticates the Client on page 113
Case 2: When the ECP is the Final Authority on page 115

Case 1: When a RADIUS Server Authenticates the Client

In this scenario, the ExtremeCloud IQ Controller redirection response includes the following:

- ExtremeCloud IQ Controller port and IP address or FQDN. The ECP can then cache this information and use it later to compose its redirection response.
- The token and WLAN ID.
- A user name and password that can be treated as the user's RADIUS credentials. These credentials must satisfy the standard requirements for RADIUS User-Name and User-Password attributes.

In order to trigger RADIUS authentication, the redirection response must not be signed.

If the appliance is configured to redirect successfully authenticated clients to their original destination, then the ECP must include in its redirection response, the "dest" parameter that was included in the appliance's redirection response.

The syntax of an unsigned ECP redirect to the appliance is:

```
[http | https]://<controller-IP-address-or-FQDN>{: <port>}/ext_approval.php?
token=<token>&wlan=<wlanid>&username=<userid>&password=<password>{&dest=<dest>}
```

Where

- {...} denotes an optional component of the URL.
- [http | https] is either "http" or "https" depending on how the WLAN service's captive portal is configured.
- :// is the literal string.
- <controller-IP-address-or-FQDN> is the appliance's IP address or Fully Qualified Domain Name. Since the appliance receives the redirect at the default HTTP or HTTPS port it does not need to be included in the redirect.
- {: <port>} is a literal colon, followed by the appliance port to which the client is redirected. The port is optional. Only include it if the port is not port 80 or port 443.
- /ext_approval.php is the literal string. It is the name of the script that is invoked on the appliance when the redirect is received there.
- <token> is the token taken from the redirect to the ECP.
- <wlanid> is the numeric identifier for the client's WLAN Service as taken from the appliance's redirect to the ECP.

- <userid> is the user name the appliance to sends to the RADIUS server to authenticate this user.
- <password> is the password associated with the given user ID.
- <dest> is the original destination the client was trying to reach, as reported in the appliance's redirect to the ECP.

The order of the parameters in the query string is not important.

Examples of the redirection from the ECP to the appliance expressed as a URL are:

```
https://10.21.15.42/ext_approval.php?token= OakRQ7uFYOH5E8dVD4PgvQ!!
&wlan=1&username=argon32&password=6Z*_aL40q!&dest=www.google.com
```

or

```
http://10.21.15.42/ext_approval.php?token= OakRQ7uFYOH5E8dVD4PgvQ!!
&wlan=1&username=argon32&password=6Z*_aL40q!
```

The parameters in the redirection response are summarized in the table below.

Table 13: Parameters in the Redirection to ExtremeCloud IQ Controller, using RADIUS authentication

Parameter Name	Parameter Value	Mandatory	Notes
wlan	Numeric String	Yes	An identifier for the WLAN Service that the client is using to access the network.
username	Alphanumeric String	Yes	The user ID is mandatory even if the URL is signed. It is used to identify the client in reports and accounting messages, even if it is not used to authenticate the client.
password	Alphanumeric String	Yes	The password is mandatory if the client is to be authenticated using RADIUS. It must be the password that the authenticating RADIUS server associates with the user ID.
dest	URL	Conditional	The dest parameter is required only if the appliance is configured to redirect the client to its original destination. The appliance directs the client's browser to an error page if it is configured to redirect to the original destination and the dest parameter is not returned to the appliance.

Related Topics

Signing the Redirection to ExtremeCloud IQ Controller on page 112
Case 2: When the ECP is the Final Authority on page 115

Case 2: When the ECP is the Final Authority

If the ECP makes the final authentication and authorization decision, it must sign the redirection response it sends to the client's browser. If it signs the redirection, it can include options that the appliance applies to the authorized client's session, including an access control role and the maximum duration for the client's session. Table 12 on page 101 lists all the parameters that can appear in a signed redirection response from the ECP, and which of them are mandatory in this case.

The syntax of an unsigned ECP redirect to the appliance is:

```
[http | https]://<controller-IP-address-or-FQDN>{:
<port>}/ext_approval.php?token=<token>&wlan=<wlanid>&username=<userid>{&dest=<dest>}
{&role=<rolename>}{&opt27=<max-seconds-duration>}&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=<Scoped-Credential>&X-Amz-Date=<YYYYMMDDThhmmssZ>&X-Amz-Expires=<duration>&X-
Amz-SignedHeaders=host&X-Amz-Signature=<signature>
```

Where

- {...} denotes an optional component of the URL.
- [http | https] is either "http" or "https" depending on how the WLAN service's captive portal is configured.
- :// is the literal string.
- <controller-IP-address-or-FQDN> is the appliance's IP address or Fully Qualified Domain Name.
- {: <port>} is a literal colon (:), followed by the TCP/IP port number to which the client is redirected. The port is optional. Include it only if the port is not port 80 or port 443.
- /ext_approval.php is the literal string. It is the name of the script that is invoked on the appliance when the redirect is received there.
- <token> is the token taken from the redirect to the ECP.
- <wlanid> is the numeric identifier for the client's WLAN Service as taken from the appliance's redirect to the ECP.
- <userid> is the user name the appliance sends to the RADIUS server to authenticate this user.
- <dest> is the original destination the client was trying to reach, as reported in the appliance's redirect to the ECP.
- <rolename> is the name of a role defined on ExtremeCloud IQ Controller that will be applied to the remainder of the client's session.
- <max-seconds-duration> is a positive integer representing the maximum duration of the client's session.
- X-Amz-Algorithm=AWS4-HMAC-SHA256 is a literal string embedded in the signed URL.
- <Scoped-Credential> is a credential in the format: <identity>/<YYYYMMDD>/world/ecp/aws4_request.
- <YYYYMMDDThhmmssZ> is the date and time at which the redirection response was sent by the ECP, in ISO 8601 compatible format.
- <duration> is a positive integer indicating the maximum duration after the X-Amz-Date that the request should be honored.

- X-Amz-SignedHeaders=host is a literal string constant.
- <Signature> is the actual signature computed over the redirection response.

The order of the parameters in the query string is not important.

The following is an example of a signed redirection response that assigns the user to a role called “Guest_Access” and limits the session duration to 10 hours:

```
https://10.10.21.6/ext_approval.php?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=BigAuthInc%2F20140729%2Fworld%2Fecp%2Faws4_request&X-Amz-
Date=20140729T153754Z&X-Amz-Expires=60&X-Amz-
SignedHeaders=host&dest=http%3A%2F%2F1.2.3.4%2Fnews.com&opt27=36000&role=Guest_Access&toke
n=T7vb1LdUZmsuY0q9V60Iww%21%21&username=test&wlan=1&X-Amz-
Signature=48389399c4b9e237ff64bbbd203a9abe272b8df513dff1eae8202df82ceb2c34
```

Table 14: Parameters that can be included in a Signed Redirection Response from the ECP

Parameter Name	Parameter Value	Mandatory	Notes
dest	URL	Conditional	The <dest> parameter is required only if the appliance is configured to redirect the client to its original destination. The appliance directs the client’s browser to an error page if it is configured to redirect to the original destination and the <dest> parameter is not returned to the appliance.
opt27 In the RADIUS protocol option number 27 is the Session-Timeout attribute.	Base 10 Number	No	The maximum amount of time, in seconds, that the current session can last before being terminated. If not specified, the default for the WLAN Service is applied to the authenticated client.
role	Alphanumeric String	No	The name of an access control role defined on ExtremeCloud IQ Controller. The appliance applies this role to the remainder of the authorized client’s session. If a role parameter is not provided, the appliance uses the default authenticated role of the VNS that the authenticated client is accessing.
token	Alpha-numeric String	Yes	An identifier for the user’s wireless session hosted on the appliance that performed the redirection.
username	Alpha-numeric String	Yes	The user name is mandatory even if the URL is signed. It is used to identify the client in reports and accounting messages, even if it is not used to authenticate the client.

Table 14: Parameters that can be included in a Signed Redirection Response from the ECP (continued)

Parameter Name	Parameter Value	Mandatory	Notes
wlan	Numeric String	Yes	An identifier for the WLAN Service that the client is using to access the network.
X-Amz-Algorithm	Alpha-numeric string	Yes	The identifier for the algorithm used to compute the “X-Amz-Signature”. This attribute must be present when the ECP is acting as the final authorizing authority. The value of this attribute is “AWS4-HMAC-SHA256” and is not configurable. The signing algorithm and the role of the identifier in it are covered in more detail in section Verify the Signed Request on page 104.
X-Amz-Credential	Alpha-numeric string	Yes	The identifier for the account whose shared secret was used to compute the “X-Amz-Signature”. Mandatory if the ECP signs the redirection response in order to act as the final authorizing authority. The credential has the format: `<identity>/<YYYYMMDD>/world/ecp/aws4_request` where: • <identity> is the identity configured for the ECP on the appliance in the WLAN Service’s ECP configuration. • <YYYYMMDD> is the year, month, and day extracted from X-Amz-Date. • world/ecp/aws4_request is a constant literal string that scopes the request.
X-Amz-Date	Alpha-numeric string	Yes	This is the date and time at which the appliance prepared and sent the redirection back to the user’s browser. The date and time are in ASCII-encoded UTC and has the format: `YYYYMMDDThhmmssZ` This attribute must be present if the ECP signs the redirection response to indicate that it is the final authorizing authority.
X-Amz-Expires	Numeric String	Yes	This is the maximum length of time in seconds that the appliance should trust the redirection response. In other words a signed redirection response from the ECP will be treated as valid only until X-Amz-Date + X-Amz-Expires. This attribute is mandatory if the ECP signs the redirection response.

Table 14: Parameters that can be included in a Signed Redirection Response from the ECP (continued)

Parameter Name	Parameter Value	Mandatory	Notes
X-Amz-Signature	ASCII-encoded hex string	Yes	This is the signature computed over some of the HTTP headers and parts of the query string, presented as ASCII encoded-hex. The field must be present if the ECP signs the request in order to act as the final authorizing authority.
X-Amz-SignedHeaders	Alpha-numeric String	Yes	Which of the headers in the HTTP request were included in the input to the calculation of the signature. This is present only when the appliance is configured sign the redirection to the ECP, in which case it must be present.

Related Topics

Signing the Redirection to ExtremeCloud IQ Controller on page 112
Case 1: When a RADIUS Server Authenticates the Client on page 113

Access Control Rules for Admin Portal Access

Configure Access Control Group on page 120
Configure Admin Access Policy Role on page 122
Configure Access Control Rule on page 123
Define Rule Precedence on page 126

Deployment Strategy

For enhanced security, the **Portal Administration** login page is now available under a proprietary URL: `<Management Interface IP Address>:8445/administration`. The previous URL: `<ICP WLAN Interface IP Address>:443/administration` is no longer supported for Admin access.

All network clients connected through a Management Port VLAN (port 5825) have access to the new port 8445. This includes the following VLANs with management access:

- The Admin Interface
- A physical interface configured with **Mgmt traffic** enabled.

To access the Admin Interface:

1. Go to **Administration** > **System** > **Interfaces**.
2. Scroll down to the list of **Interfaces**.

To access Bridged@AC VLANS with **Mgmt traffic** enabled:

1. Go to **Configure** > **Policy** > **VLANs** > **Add**.
2. Select **Layer 3**.
3. Select **Mgmt traffic**.

Additionally, you can configure Access Control Rules to filter client access and limit exposure to the Admin portal by associating members of the Admin group to port 8445. This deployment strategy involves configuring: Access Control Groups, policy roles, and captive portal definitions to define an Access Control Rule for Admin access.

From ExtremeCloud IQ Controller, take the following steps:

1. Create an Access Control Group.
2. Create a Policy Role with Layer 3 and Layer 4 rule definitions.
3. Create a Captive Portal definition or specify the Default captive portal.
4. Create an Access Control Rule for Admin access.
5. Place the Access Control Rule for Admin access within the **Rules List**.

Related Topics

Configure Access Control Group on page 120
Configure Admin Access Policy Role on page 122
Configure Access Control Rule on page 123
Define Rule Precedence on page 126
Default Access Control Groups on page 121

Configure Access Control Group

To configure an Access Control Group, take the following steps:

1. Go to **Onboard** > **Groups** > **Add**.
2. Configure the following Access Control Group settings and select **Save**.

   The entry parameters depend on the Group Type.Table 15 describes each setting and provides an example value configured for the Access Control Group.

Table 15: Access Control Group Settings

Field	Description
Name	Group name. Example: **Captive Portal Admins**
Description	Description of the group. **Allows Self Registration**.
Group Type	Criteria by which the accounts are grouped. Example: **End System — MAC**
Group Mode	For End System LDAP User Groups only — Specify whether to match any or match all of the LDAP attributes. Valid values are: • Match All • Match Any Example: **Match Any**
Group Entries	A list of entries for the Group Type. Example: **End System — MAC**. Use the **Search** field to search for an entry.

Figure 38: Access Control Group Configuration: Captive Portal Admins

Next, review the Default Access Control Groups, then we will create an Admin access policy role.

Related Topics

Default Access Control Groups on page 121
Configure Admin Access Policy Role on page 122

Default Access Control Groups

The following Access Control system groups are provided with the ExtremeCloud IQ Controller installation by default.

- Blacklist. A list of MAC addresses that are prohibited from accessing the network.
- Registered Guests. A list of MAC addresses that have been granted access to the network via the Guest captive portal.
- Registration Denied Access. A list of MAC addresses that have been denied access to the network.
- Registration Pending Access. A list of MAC addresses that are waiting permission to access to the network.
- Web Authenticated Users. A list of MAC addresses that have been granted access to the network via the Authenticated captive portal.
- DFNDR_PolicyGeneration. Default Group created for Extreme Defender Application. Allows Defender Policy Generator to move clients to and from build roles.

In addition, the following Device Type groups are provided with your ExtremeCloud IQ Controller installation:

- Windows
- Windows Mobile
- Linux
- Mac
- iPhone
- BlackBerry
- Android
- Windows
- Mobile Game Console
- Chrome OS

You cannot delete system groups.

Related Topics

Define Rule Precedence on page 126

Configure Admin Access Policy Role

Configure a Policy Role that allows Admin access to the captive portal **Admin** page using **Port 8445**. Table 16 on page 122 describes each setting and provides an example value configured for the Captive Portal Admin Role.

1. Go to **Configure** > **Policy** > **Role** > **Add**.
2. Configure the following Role settings:

Table 16: Role Parameter Settings

Field	Description
Name	Name of the Policy Role. Example: **Captive Portal Admin**
Bandwidth Limit	Select this option to allow unlimited bandwidth. Select to set the Class of Service value.
Default Action	Determines the access control default action. If you do not define policy rules for a role, the role's default action is applied to all traffic subject to that role. Policy Rules affect traffic that meets the filter criteria. Example: For Role **Captive Portal Admin** the Default Action is **Deny**. Deny packets that do not match a filter rule or deny packets when a filter rule does not exist. When a packet *does* match the filter rule action Allow packet using the specified VLAN **GTAC (222)**.
VLAN ID	Policy roles default to the VLAN specified during network configuration. You can specify a unique VLAN here. Select to add a new VLAN option. Example: **GTAC (222)**
Associated Profile	Indicates profiles that this role is associated with. In our example, **Role is not associated with a Profile**.
Rules	Specify the following L3 L4 Rule: Example: Allow traffic from IP/Subnet **22.222.2./32** through Port **8445**.

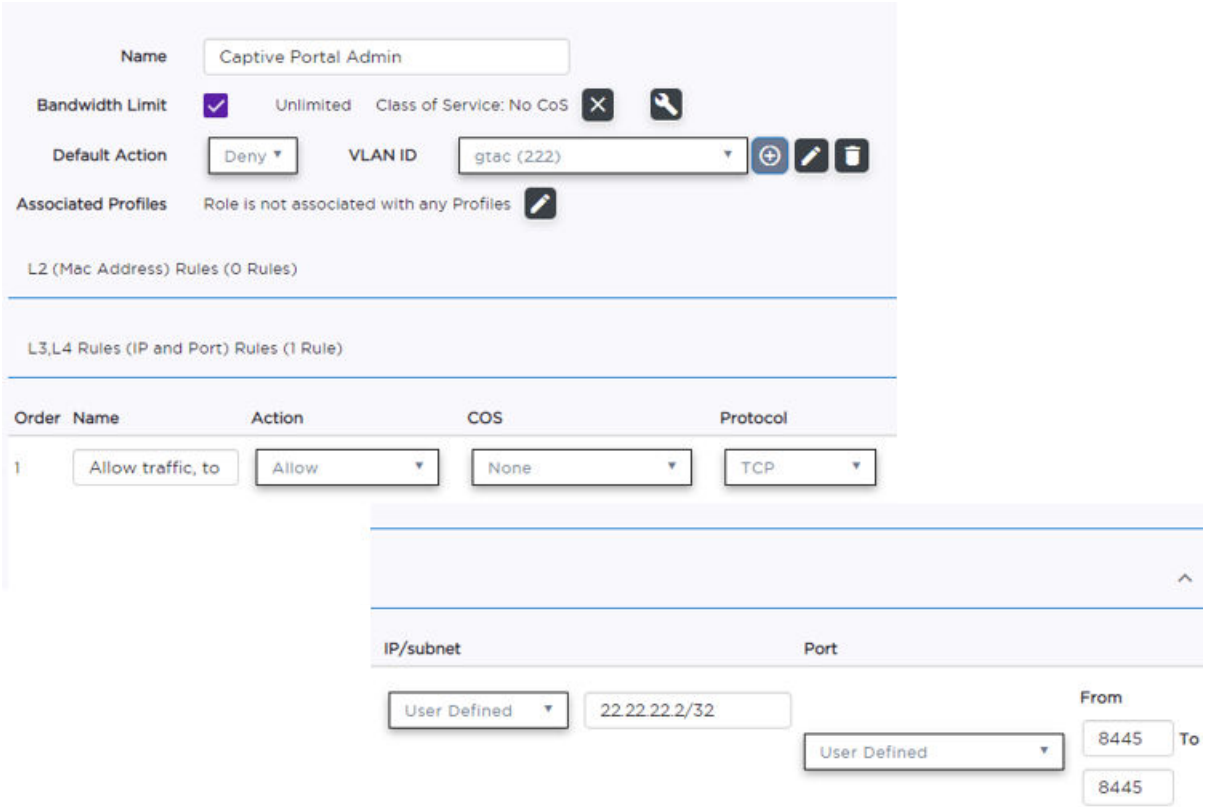


Figure 39: Admin Access Policy Rule Configured for Port 8445

Next, configure the Access Control Rule.

Related Topics

Configure Access Control Rule on page 123

Configure Access Control Rule

An Access Control Rule is used to further define an end user's network access based on the groups and policy roles with which the end user is associated.

To configure an Access Control Rule, take the following steps:

1. Go to **Onboard** > **Rules** > **Add**.

2. Table 17 describes each setting and provides an example value configured for the Access Control Rule. Configure the following rule settings:

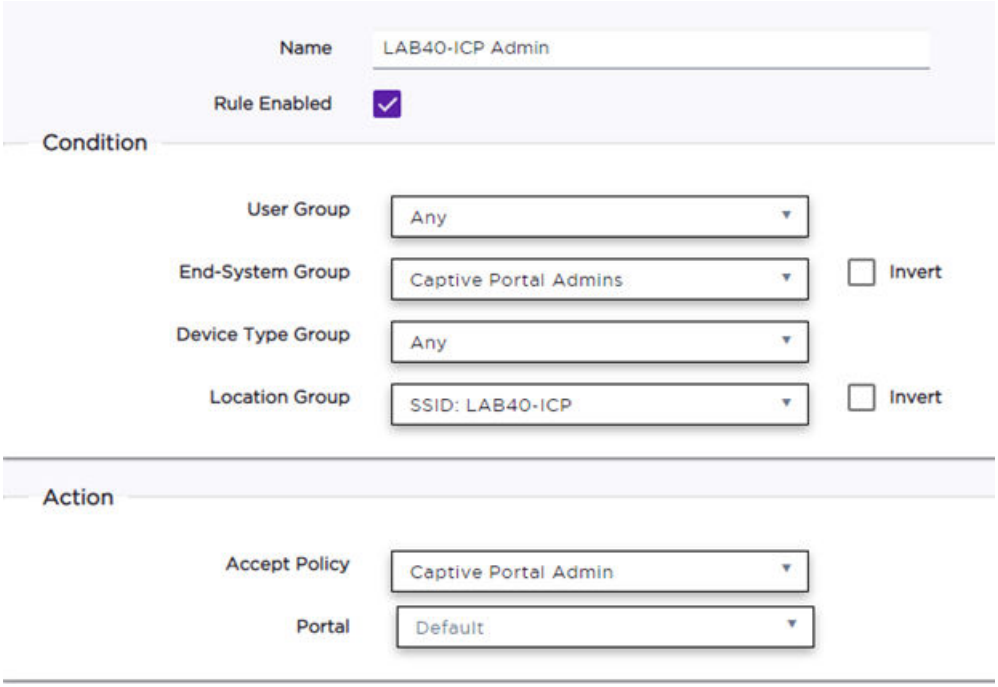


Figure 40: Access Control Rule Configuration: Captive Portal Admins

Table 17: Access Control Rule Settings

Field	Description
Name	Rule name. Example: **Lab40-ICP Admin**
Rule Enabled	Check to enable this rule.
Conditions Note: • If you select **Any**, then the criteria is ignored during the rule match process. • If you select the **Invert** check box, it is considered a rule match if the end-system *does not* match the selected value.	
User-Group	**Any**. No specific group configured.
End-System Group	The end-system group that you configured in Configure Access Control Group on page 120 (**Captive Portal Admins**). End-systems that do not match any of the listed rules are assigned the Default Catchall rule.
Device Type Group	**Any**. No specific group configured.
Location Group	The location group that you configured that is affected by the rule. **SSID: Lab40-ICP**

Table 17: Access Control Rule Settings (continued)

Field	Description
Accept Policy	Associate a policy role with the Access Control Rule. Example: **Captive Portal Admin**. We configured this policy under Configure Admin Access Policy Role on page 122. The Default Action is defined in the policy rule.
Portal	Associate a captive portal with a rule. Our example uses the **Default**.

Next, review the Default Access Control Rules, then go to **Onboard** > **Rules** to define the rule precedence of the Access Control Rules.

Related Topics

Default Access Control Rules on page 125
Define Rule Precedence on page 126
Configure Access Control Group on page 120
Configure Admin Access Policy Role on page 122

Default Access Control Rules

The following Access Control Rules are added when you enable an internal captive portal. The rules are removed when you disable the captive portal.

- Blacklist. This rule quarantines any MAC address that is part of the Blacklist group. This is always the first rule in the **Rules List**.
- Default Catchall. This rule applies the Default Auth Policy to any MAC Address. It is always the final rule in the **Rules List**.
- Unregistered: This rule is a catchall, and will always be listed immediately before the Default Catchall. Users who do not match any other rule will match Unregistered, and they will be presented with the captive portal.
- Registered Guests: Users who complete registration through the Guest captive portal will match this rule, which checks for end-system MAC addresses in the Registered Guests group.

  Note
  This rule is only present when Guest Registration or Guest Web Access is enabled.

- Web Authenticated Users: Users who complete registration through the Authenticated captive portal will match this rule, which checks for end-system MAC addresses in the Web Authenticated Users group.

  Note
  This rule is only present when Authenticated Registration or Authenticated Web Access is enabled.

Related Topics

Configure Access Control Rule on page 123

Define Rule Precedence

The order of the Access Control Rules matter. Rules are evaluated from the top down. Figure 41 displays an example Rules List. The rules are evaluated in order.

To access the **Rules List**, go to **Onboard** > **Rules**.

Rules

Enabled	Name	Conditions	Accept Policy	Portal
✓	Blacklist	End-System is in **Blacklist**	Quarantine	Default
✓	LAB40-ICP Admin	End-System is in **Captive Portal Admins** and Location is in **SSID: LAB40-ICP**	Captive Portal Admin	Default
✓	Registered Guests Loc: Network: LAB40-ICP	End-System is in **Registered Guests** and Location is in **Network: LAB40-ICP**	Guest Access	Default
✓	Unregistered Loc: Network: LAB40-ICP	Location is in **Network: LAB40-ICP**	Unregistered role for LAB40-ICP	Default
✓	Unregistered Loc: Network: LAB40-ECP	Location is in **Network: LAB40-ECP**	Unregistered role for LAB40-ECP	Default
✓	Default Catchall		Use Default Auth Role	Default

Figure 41: Access Control Rules List Order

In the following example, the MAC Address evaluates the following rules:

- Member of the **Blacklist** Group?
  - Yes. MAC Address Quarantined.
  - No. Evaluate next rule.
- Member of the **Captive Portal Admin** Group?
  - Yes. Go to the captive portal Administration page.
  - No. Evaluate next rule.
- Member of the **Registered Guests** Group?
  - Yes. Present Captive Portal.
  - No. Evaluate next rule.
- Unregistered Guest on Network **Lab40-ICP**?
  - Yes. Present Captive Portal.
  - No. Evaluate next rule.
- Unregistered Guest on Network **Lab40-ECP**?
  - Yes. Present Captive Portal.
  - No. Evaluate next rule.
- **Default Catchall** Rule.
  - Access Denied

Related Topics

Default Access Control Groups on page 121

Centralized Web Authorization

CWA with ISE Deployment on page 128
CWA with ExtremeControl Deployment on page 145

Deployment Strategy

Centralized Web Authentication (CWA) provides the URL for the captive portal dynamically through RADIUS attributes, following the successful authentication over 802.1x. CWA can integrate with both an ExtremeControl captive portal server and a Cisco® ISE captive portal server.

The configuration required on ExtremeCloud IQ Controller is the same regardless of the captive portal server used:

On ExtremeCloud IQ Controller:

1. Configure a AAA Policy, defining the RADIUS server, then reference that AAA Policy on the CWA captive portal network configuration.

   The RADIUS server in the AAA Policy is the authentication server that sends the redirection attribute back to ExtremeCloud IQ Controller. You only need the role name on ExtremeCloud IQ Controller to match the Filter-ID sent in the RADIUS-Accept.
2. Configure a CWA captive portal network.
3. Configure a Redirect Policy **Role** that includes at least one redirect rule.

When integrating with an ExtremeControl server, we use the ExtremeControl rules engine. The rules engine assigns the policy **Unregistered** to the redirection and assigns the policy **Enterprise User** when authenticated by the captive portal:

1. Map the redirection policy that you created on ExtremeCloud IQ Controller to ExtremeControl.
2. Create an allow policy on ExtremeCloud IQ Controller and map it to ExtremeControl.

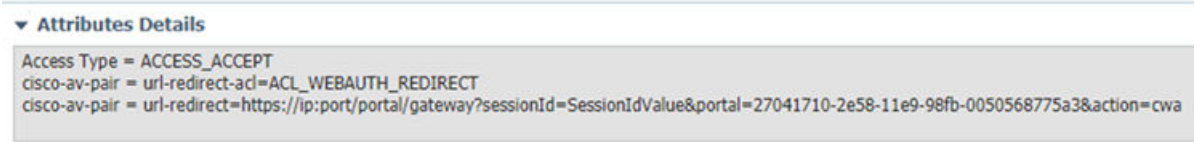
When integrating with a Cisco® ISE captive portal server:

1. Configure an Authorization Profile that references the policy role configured on ExtremeCloud IQ Controller.
2. Configure an Authorization Policy that references the Authorization Profile.

The Authorization Policy will include three profiles: the Redirection Profile, an Allow Profile, and a Deny Profile.

Note
The Allow Role will take effect once the user has been successfully authenticated to the network. From the clients list on ExtremeCloud IQ Controller, you can view the client that authenticated the network. The Allow Role is listed in the Role column.

3. The Authorization Profile generates the following attribute details:
   - The redirection policy role.
   - The redirection URL.



Related Topics

CWA with ISE Deployment on page 128
CWA with ExtremeControl Deployment on page 145
AAA Policy Settings for CWA on page 131

CWA with ISE Deployment

This section outlines the configuration settings for Centralized Web Authentication (CWA) integration with Cisco ISE captive portal server.

Related Topics

AAA Policy Network Configuration — ISE on page 128
CWA Network Settings — ISE on page 136
CWA Policy Redirection Role — ISE on page 139
Configure Authorization Policy on Cisco® ISE Server on page 141

AAA Policy Network Configuration — ISE

You can create a AAA Policy that can be referenced through a WLAN Service, bypassing the local Network Access Control on ExtremeCloud IQ Controller.

Note
AAA Policy can only be configured for WLAN networks requiring MACAUTH, External Captive Portal, or EAP.

To configure a AAA network policy:

1. Go to **Configure** > **Networks** > **WLANs** and select a network.

   AAA Policy is displayed for WLAN Networks that require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the ExtremeCloud IQ Controller. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal.
2. Select an **Auth Type**.

   The AAA Policy field displays.

3. From the AAA Policy field, select ⊕ to add a new policy, or select ◪ to edit a policy.

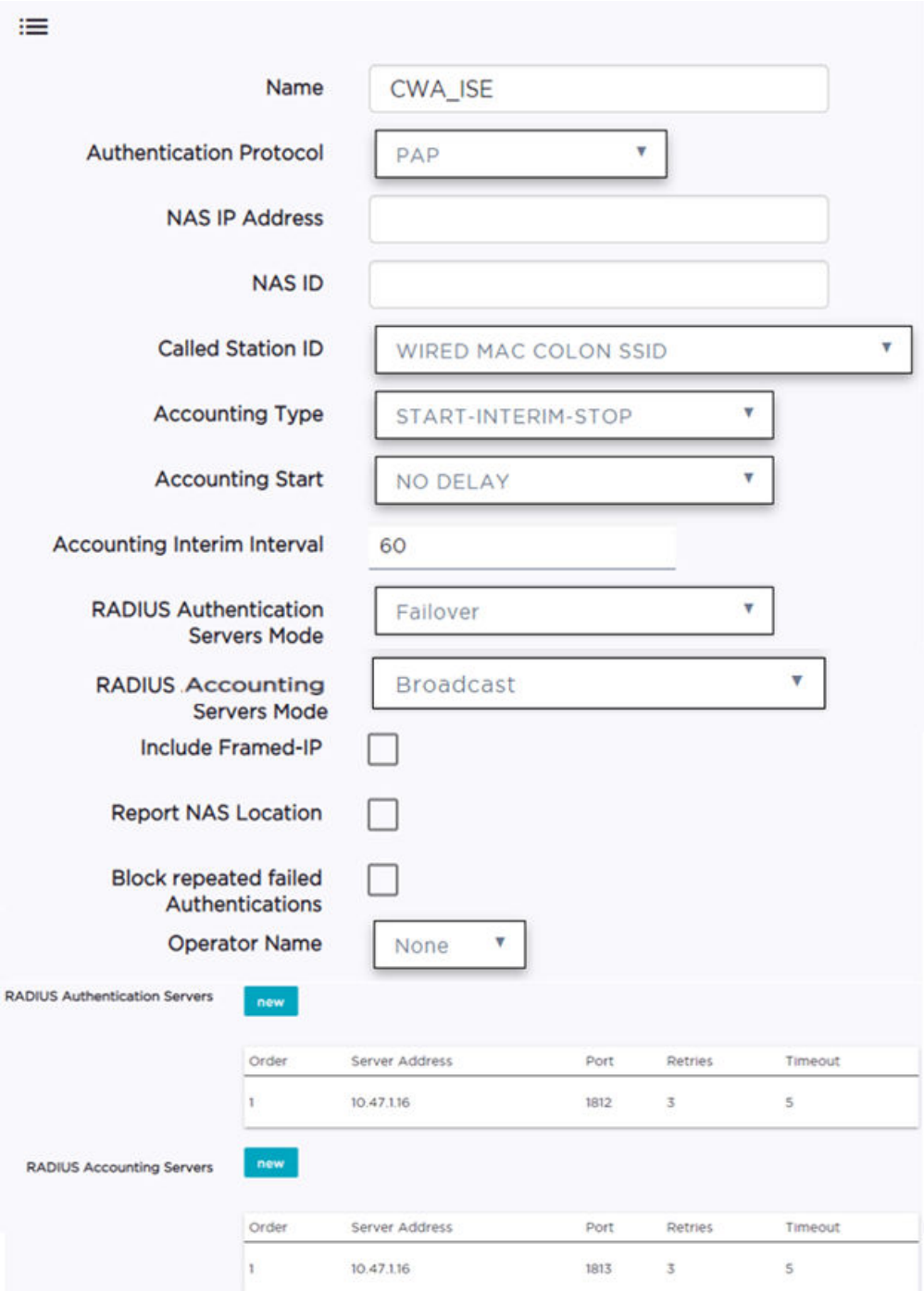


Figure 42: Centralized Web Authentication AAA Policy

4. Configure the AAA Policy settings.

Related Topics

AAA Policy Settings for CWA on page 131
RADIUS Settings on page 135

Centralized Web Authorization on page 127
CWA Network Settings — ISE on page 136
CWA Policy Redirection Role — ISE on page 139
Configure Authorization Policy on Cisco® ISE Server on page 141

AAA Policy Settings for CWA

Details about AAA Policy settings for CWA:

Name

Policy name.

Authentication Protocol

Authentication protocol type for the RADIUS server (PAP, CHAP, MS-CHAP, or MSCHAP2).

Call Station ID

Identifies a group of access points. The Call Station ID is often configured in a large network using an external NAC or RADIUS server. Possible values are:

- Wired MAC: SSID
- BSSID (APs supported on a Centralized site only)
- Site Name
- Site Name: Device Group Name
- AP Serial Number

Note
Call Station ID allows for Zone authentication with a Centralized site.

- Site Campus
- Site Region
- Site City

Accounting Type

Determines when the appliance generates the accounting request. Valid values are:

- Start-Interim-Stop — Start record after successful login by the wireless device, interim record, and an accounting stop record based on session termination.
- Start-Stop — Start record after successful login by the wireless device user and an accounting stop record based on session termination.

The appliance sends the accounting requests to a remote RADIUS server.

Wait for client IP before starting accounting procedure

By default, the Accounting Start record is generated when the client is authenticated. Enable this setting to generate the Accounting Start record when the client acquires a non local IP address. Use this option for captive portals, which use RADIUS Accounting to learn of the client IP address before providing the landing page.

Accounting Interim Interval

The number of seconds (60-3600) between each interim update for a specific session. Default value is 60.

RADIUS Authentication Servers Mode

Note
Not applicable when **NAI Routing** is enabled.

Select the availability behavior for RADIUS servers. Valid values are: **Failover** or **Load Balance**.

AAA Policy supports the ability to load balance RADIUS requests across target servers in a load-balancing pool. (A minimum of two servers is required.) Each client authentication session begins and ends on a single RADIUS server. The ExtremeCloud IQ Controller validates that each server can be reached and logs an alert when a server in the pool is unreachable. The server pool is readjusted based on the status of each server in the pool.

Note
Configure one server for both Accounting and Authentication purposes.

When this setting is set to **Failover**, a RADIUS request is sent to one server at a time:

- The RADIUS request is sent to the Primary server (based on the RADIUS server order in the AAA policy).
- When the Primary server is not accessible, the request is sent to the second server (the Failover server).
- When the Primary server is accessible, the request is automatically sent to the Primary server instead of the Failover server.

  Note
  The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

When this setting is set to **Load Balance**, a RADIUS request is sent in round robin fashion:

- When a RADIUS server is not accessible, ExtremeCloud IQ Controller stops sending requests to that server.
- When a server is accessible, the server is added to the pool of servers.

  Note
  The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

Note
There is no correlation between the RADIUS server that is used for authentication and the RADIUS server that is used for accounting.

RADIUS Accounting Servers Mode

Note
Not applicable when **NAI Routing** is enabled.

Determines the server selection mode when accounting packets are sent to a single server. When the selected accounting server does not respond to the accounting requests, the accounting packets are sent to the next configured accounting server. The selection applies to all Services and to all sites on ExtremeCloud IQ Controller.

- **Round-Robin** — The server is selected on a round-robin basis starting at the top of the list of approved servers. The first server is used until it fails, and that pattern continues down the list. When the last server fails, then the first server is used again.
- **Broadcast** — RADIUS accounting packets are sent to all configured accounting servers in the AAA Policy.

  For controllers in an availability pair, the primary and backup servers must be synchronized when the WLAN Services are synchronized. If the primary server has failed resulting in a backup server being used for authentication, the controller periodically sends a "Health Check" to the primary server to see if it has recovered. If the primary server has recovered, the controller starts using the primary server for all new authentications. All authentications in progress continue to use the backup server.

Note
There is no correlation between the RADIUS server that is used for authentication and the RADIUS server that is used for accounting.

Report NAS Location

Sends Network Access Server (NAS) Location per the RFC5580 Out of Band agreement. After a NAS Location change, the new NAS Location is reported in the next RADIUS Request or RADIUS Accounting message.

Note
Mid-session requests and the Initial Server Request for Location as described in RFC5580 are not supported.

The following additional attribute value pairs (AVP) used by RFC5580 are supported:

- LOCATION-INFO
- LOCATION-DATA

  Note
  Site Location details are reported in LOCATION-DATA. For more information on Site Location information, see the ExtremeCloud IQ Controller User Guide.

- BASIC-LOCATION-POLICY-RULES
- OPERATOR-NAME (Described below)

Override Reauthentication Timeout

Enable this setting to override the reauthentication period that is returned by the RADIUS server. When reauthentication is enabled, the timeout value that is returned by the RADIUS sever is overwritten with the value that is specified here. Valid values for the Override Reauthentication Timeout are 60-300 seconds.

Block repeated failed Authentications

Enable this setting to minimize the RADIUS server load that is created by repeated authentication requests and failures. Authentication requests from a client are blocked for a configurable period of time. While blocked, RADIUS requests from the client are ignored. This setting applies to a specific WLAN. The client can continue to send authentication requests on a different WLAN.

Consecutive failed Authentications must be received at the ExtremeCloud IQ Controller in the **Elapsed time for failed Authentications (Seconds)** for the **Quiet Timeout (Seconds)** to start. After the quiet timeout expires, the client's RADIUS requests are forwarded to the RADIUS server again.

When enabled, the following settings display:

Consecutive failed Authentications

The number of failed authentication attempts. Valid values are 1 to 10. Default value is 5.

Elapsed time for failed Authentications (Seconds)

The threshold in seconds that determines if the client authentication requests are blocked. This is the window of time in which the failed authentication attempts occur. Valid values are 1 to 10 seconds. The default value is 3 seconds.

Quiet Timeout (Seconds)

The amount of time that authentication requests from the client are blocked before its RADIUS requests are forwarded to the RADIUS server again. Valid values are 1 to 300 seconds. The default value is 300 seconds (5 minutes).

By default, if 5 attempts are made within 3 seconds, the client authentication requests are blocked for 300 seconds (5 minutes), and RADIUS requests from that client are ignored. After 5 minutes, client RADIUS requests are forwarded to the RADIUS server again.

Note
In Failover mode, the Deny list is published to the peer ExtremeCloud IQ Controller.

Operator Name

RADIUS attribute composed of the operator namespace identifier and the operator name. The combination of operator name and namespace identifier uniquely identifies the owner of an access network. The Operator Name cannot exceed 253 bytes. Valid values are:

- Tadig — Three-character Country Code followed by a two- character alphanumeric operator ID
- Realm — Registered Domain Name of Operator
- E212 — Mobile Country Code or Mobile Network Code

- OneCC — Three-character Country Code followed by 1-6 uppercase ITU Carrier Codes
- WBAID — Used with a WBA OpenRoaming AAA policy that is automatically generated when using an OpenRoaming Hotspot. For more information on Hotspot, see the ExtremeCloud IQ Controller User Guide.
- None

RADIUS Authentication Servers

Note
Not applicable when **NAI Routing** is enabled.

To add RADIUS servers for authentication, select **Add**. You can configure up to four RADIUS servers for authentication.

We have the CWA server configured.

RADIUS Accounting Servers

Note
Not applicable when **NAI Routing** is enabled.

To add RADIUS servers for accounting, select **Add**. You can configure up to four RADIUS servers for accounting.

We have the CWA server configured.

RADIUS Settings

Configure the following parameters, and then select **Save**.

Peer Discovery (RFC 7585) Enabled

Select this option to enable peer discovery.

Peer Discovery uses the Network Access Identifier (NAI) in the UserName attribute of the RADIUS packet to dynamically discover the RADIUS server using DNS.

It is supported for Secure(TLS) servers only; therefore, Peer Discovery defaults to the **Type** value = Secure. Both the server IP address and port values are dynamically discovered. The port is usually TCP 2083.

Type

Select between **Standard** (UDP) or **Secure** (RADSEC) protocol.

RADSEC supports RADIUS transactions conducted securely over TCP and TLS (RFC 6614). RADSEC is not supported with Local Onboarding, and it is not available with ADMIN access.

Server Address

The RADIUS server address. This value cannot be changed.

Port

- A User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic. Select a UDP port number for standard protocol security.
- For a secure RADSEC protocol, use port **2083** This is the default port.

Trust Point

Refers to the certificate file required for the secure RADSEC protocol. When a secure RADSEC protocol is configured, the certificate file of the Access Network Provider (ANP) and its private key must be specified, and the CA must also be specified to authenticate the peer's certificate. Select from the list of configured Trust Points. For information about configuring Trust Points, . see Trust Points in the *User Guide*.

Retries

Determines the number of times ExtremeCloud IQ Controller will attempt to authenticate an end user.

For Local Onboarding, use the **Retries** and **Timeout** values with the **RADIUS Server Health Check** parameters to detect RADIUS servers that are not responding and fail over to a second server if necessary. When Local Onboarding bypassed is enabled, all RADIUS requests are sent to one RADIUS server until it fails; then, the next RADIUS server is used.

Timeout

Determines a timeout value, in seconds, for the RADIUS server connection.

Status Server Request Timeout

Status Requests are sent by the RADIUS client to query the status of the RADIUS server. The Status Request Timeout is the period between two successive status requests . Status requests are only sent when the RADIUS server has stopped responding to the Access Request with an Access Response.

Shared Secret

The password that is used to validate the connection between the client and the RADIUS server.

For RADSEC, **radsec** is the default password.

Mask

Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

CWA Network Settings — ISE

To configure a Centralized Web Authentication (CWA) captive portal:

1. Go to **Configure** > **Network** > **WLANS**.

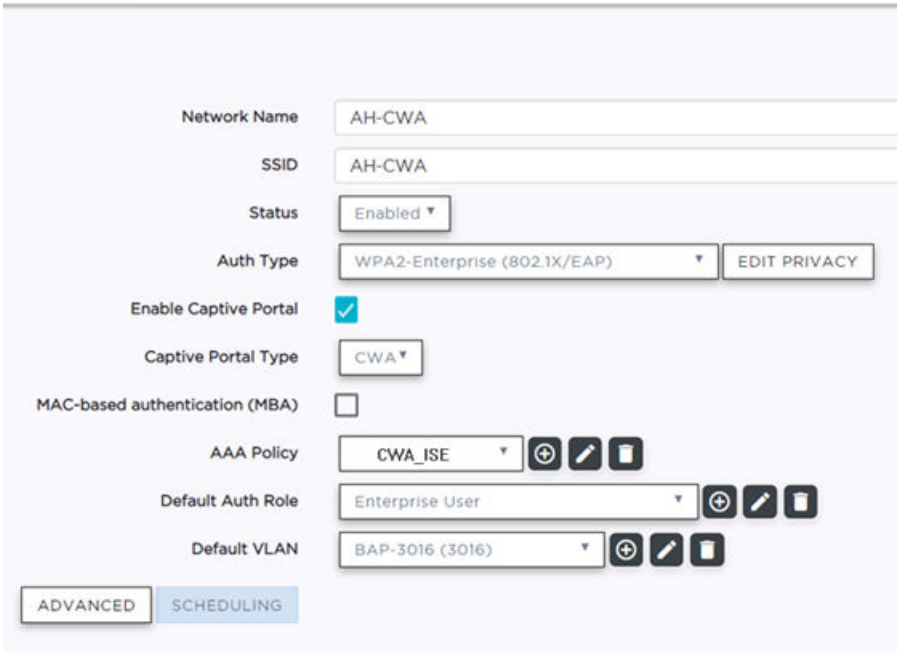


Figure 43: CWA Network on ExtremeCloud IQ Controller

2. Configure the following settings:

Table 18: Centralized Web Authentication Network Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Maximum 32 characters. Upper and lowercase allowed. Example: PermanentStaff
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.
Auth Type	The Authorization Type for a CWA captive portal must be **WPA2 Enterprise (802.1x EAP)**
Enable Captive Portal	Select this option to configure a captive portal network.

Table 18: Centralized Web Authentication Network Settings (continued)

Field	Description
MAC-Based Authentication	(Optional) Select this option to enable MBA. When selected, multi-factor authentication is enabled. The following parameter displays when MAC-based Authentication is enabled: • **MBA Timeout Role**. Select the role that will be assigned to a wireless client during MAC-based authentication (MBA) if the RADIUS server access request times out. If no MBA Timeout Role is selected, then a RADIUS server timeout is treated like an Access-Reject, which prevents the client from accessing the network. Other options: ◦ — create a new role ◦ — edit role ◦ — delete role
Captive Portal Type	**CWA**
AAA Policy	Specify the AAA Policy associated with the captive portal. Define the RADIUS server used for authentication in the AAA Policy. This is the IP address of the captive portal. See Figure 44 on page 139.
Default Auth Role	Specify the default authorization role that is configured on ExtremeCloud IQ Controller.
Default VLAN	Specify the default VLAN that is configured on ExtremeCloud IQ Controller.

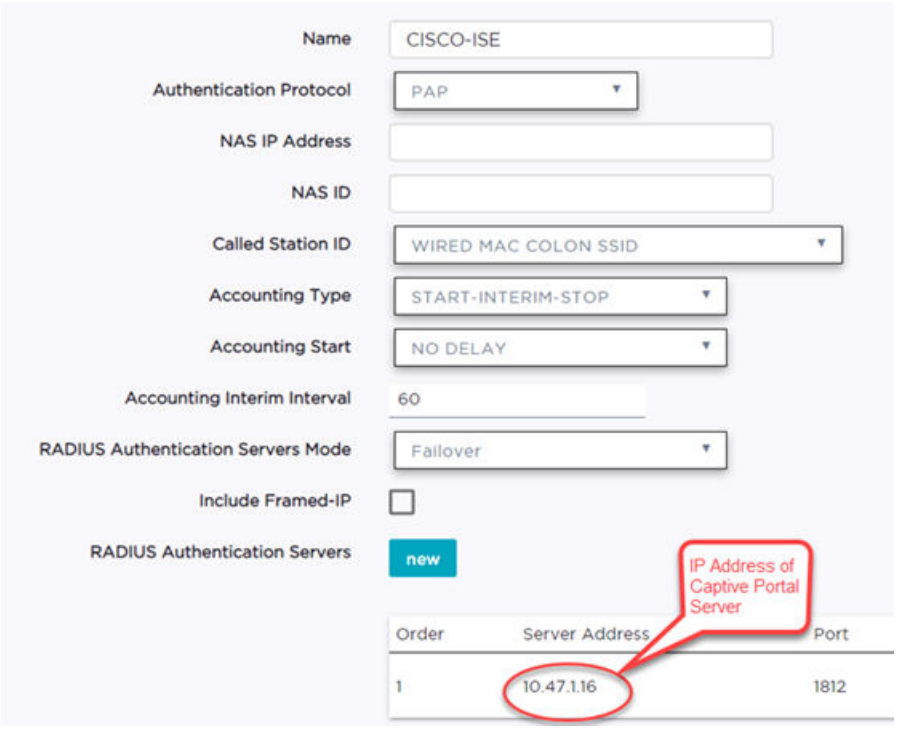


Figure 44: AAA Policy for CWA — RADIUS Server definition

For more information about creating policy roles or configuring VLANs, see the *ExtremeCloud IQ Controller User Guide*.

Related Topics

AAA Policy Network Configuration — ISE on page 128
CWA Policy Redirection Role — ISE on page 139

CWA Policy Redirection Role — ISE

To configure a policy role with at least one redirection rule:

1. Go to **Configure** > **Policy** > **Role** > **Add**.
2. Create a new role.
   - ACL_WEBAUTH_REDIRECT is the example redirection role for the Cisco® captive portal server.
3. Select **Layer 3/Layer4** and configure the parameters for a redirect rule that works with CWA captive portal. See Table 19 on page 140.

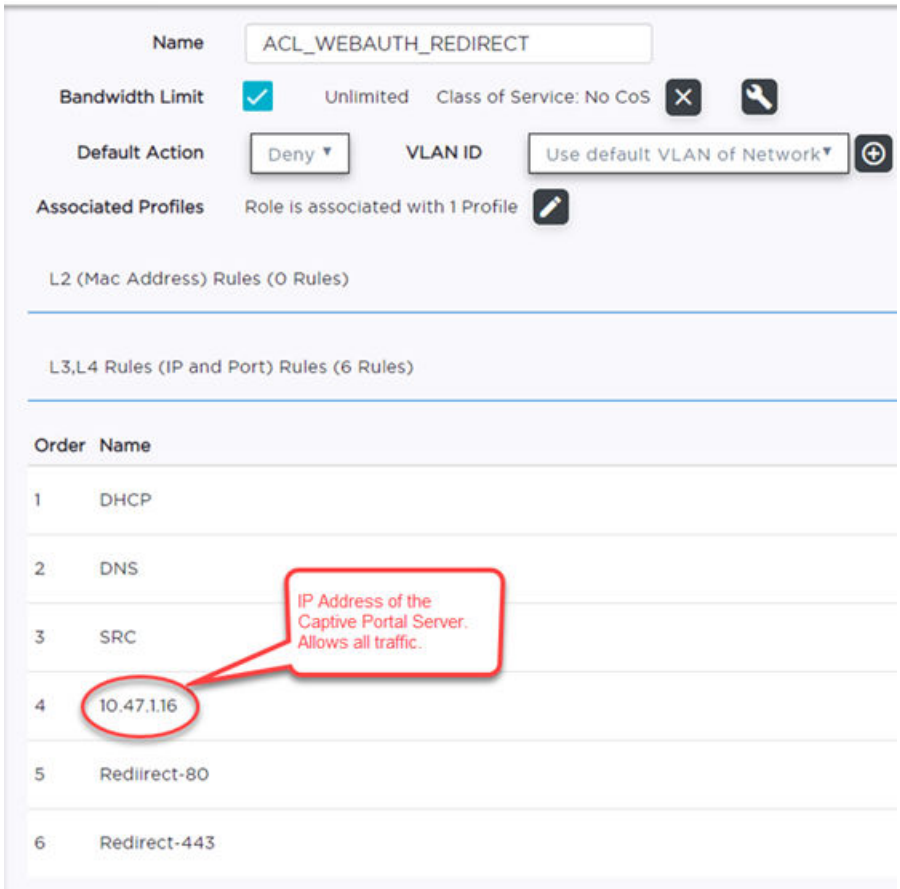


Figure 45: Example Redirection Role on ExtremeCloud IQ Controller that includes six L3/L4 rules

Figure 46: Redirect-80 rule redirects HTTP traffic from Port 80

Table 19: Rule Configuration for Layer3/Layer4 Redirection Rules

Field	Description
Name	Provide a name for the rule. Example: **Redirect-80** that redirects traffic on HTTP port 80.
Action	**Redirect**
Protocol	**TCP**
IP/Subnet	**User-Defined**. Then specify the IP address of the captive portal. The redirection role includes a rule that points to the CWA server IP address.
Port	Include at least one rule for HTTP port 80 or HTTPS port 443 The redirection role includes a rule for both HTTP port 80 and HTTPS port 443

For more information about creating policy roles, see the *ExtremeCloud IQ Controller User Guide*.

Related Topics

Centralized Web Authorization on page 127
AAA Policy Network Configuration — ISE on page 128
CWA Network Settings — ISE on page 136
Configure CWA on ExtremeControl on page 154
Configure Authorization Policy on Cisco® ISE Server on page 141

CWA Server Configuration — ISE

Configure an Authorization Policy on the CWA server to integrate with ExtremeCloud IQ Controller. From the CWA server, you configure the redirect policy to return the specific redirect rule that you configured on ExtremeCloud IQ Controller. The CWA Authorization Policy on the CWA server includes three profiles: the Redirection Profile that is referenced from ExtremeCloud IQ Controller, an Allow Profile, and a Deny Profile.

CWA integrates with a captive portal on a Cisco ISE server. The following topics outline how to configure the captive portal server:

- Configure Authorization Policy on Cisco® ISE Server on page 141

Configure Authorization Policy on Cisco® ISE Server

Configure Centralized Web Authentication (CWA) to integrate with a Cisco® ISE server:

1. Configure the Authorization Profile (`CWA_WebAuth`) on the Cisco® ISE server. This profile references the role (`ACL_WEBAUTH_Redirect`) that was configured on ExtremeCloud IQ Controller.
   a. Go to **Policy** > **Policy Elements** > **Results**.
   b. Select **Authorization** > **Authorization Profiles**.

   We have configured `CWA_WebAuth`. Notice the reference to the policy rule configured on ExtremeCloud IQ Controller: `ACL_WEBAUTH_Redirect`.

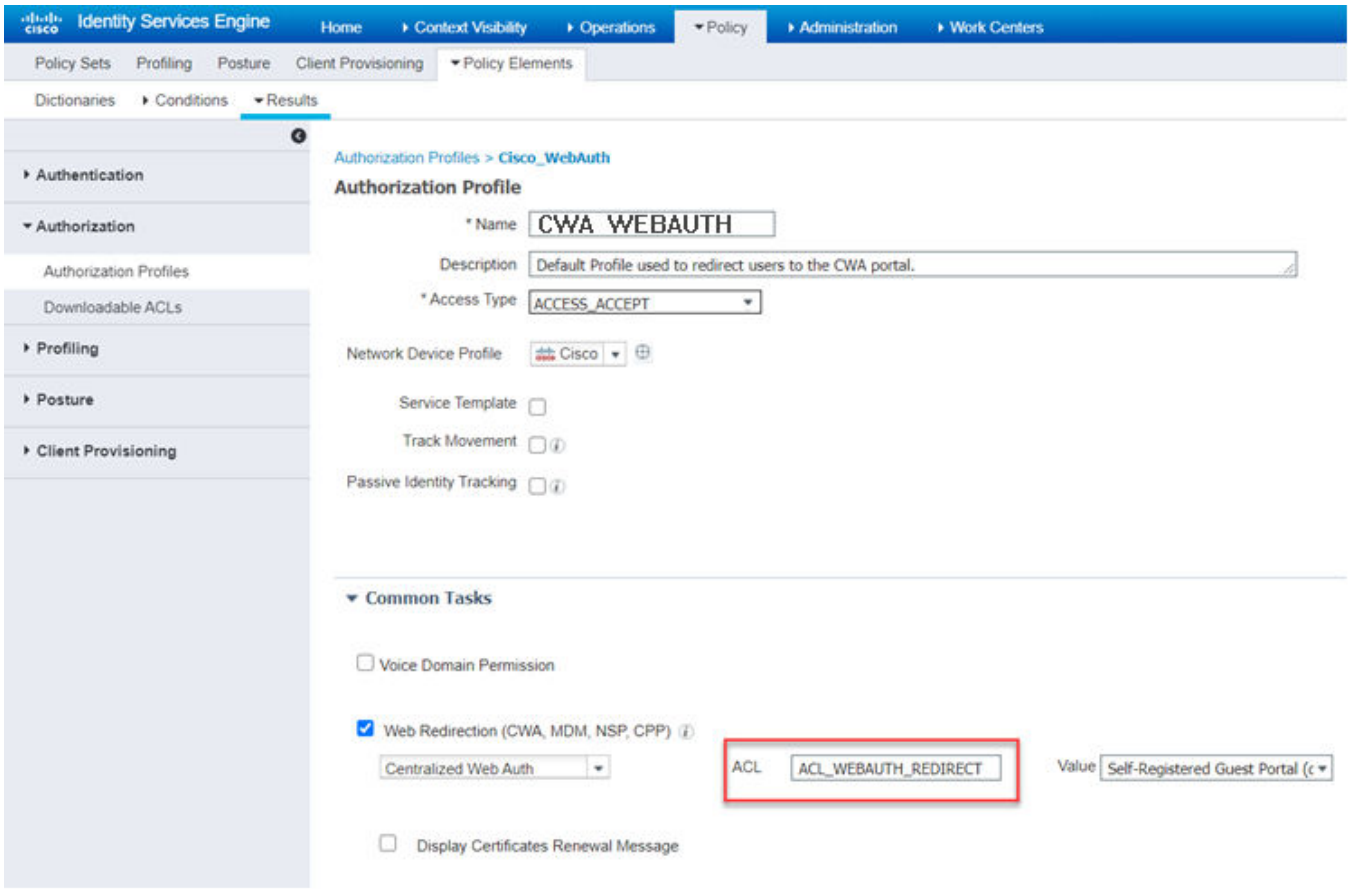


Figure 47: CWA_WebAuth Authorization Profile Configuration

2. Define the policy set.

   Go to **Policy** > **Policy Set**. We have configured `AH-CWA`. The Policy Set includes the Authorization Profile `CWA_WebAuth` that was configured in Step 1.

   Add an Authorization Policy that includes the condition: `Radius-Called-Station-ID - Contains - x`, where x is the SSID of the network. The Authorization Policy assigns the Authorization Profile (CWA_WEBAUTH) that references the redirection Role on ExtremeCloud IQ Controller (ACL_WEBAUTH_REDIRECT).

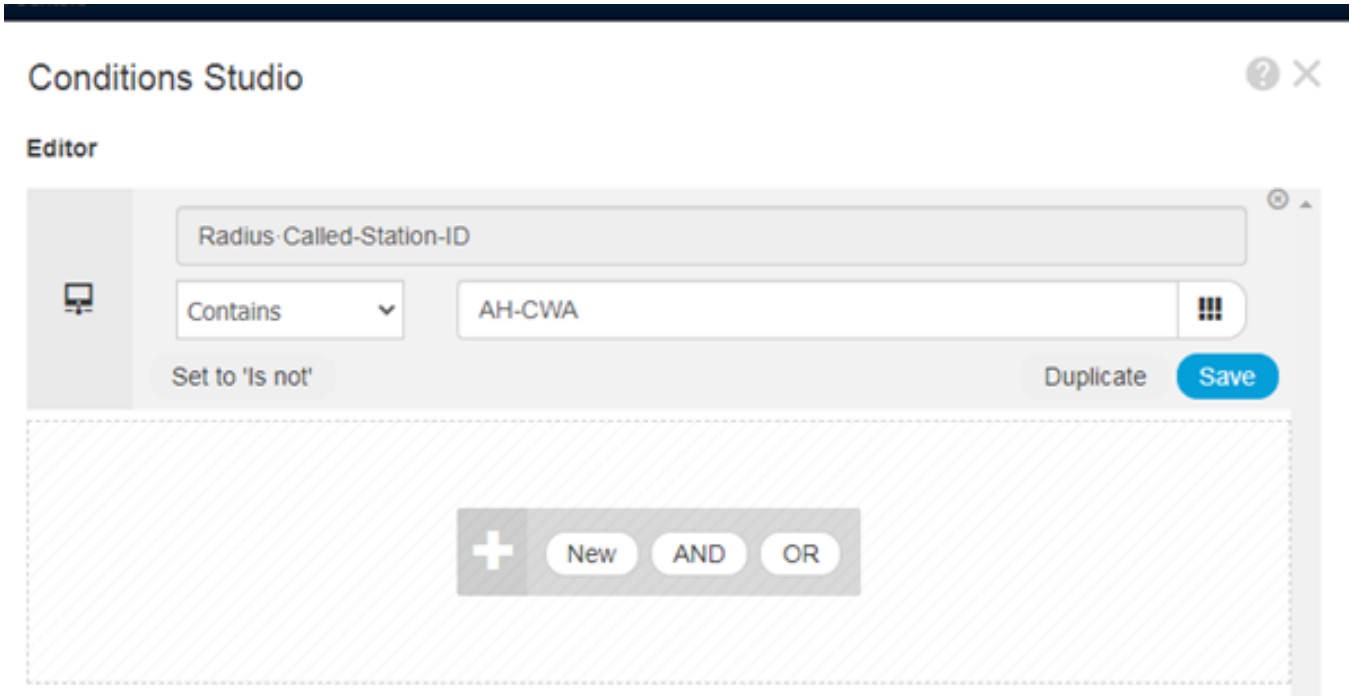


Figure 48: Condition to match on SSID

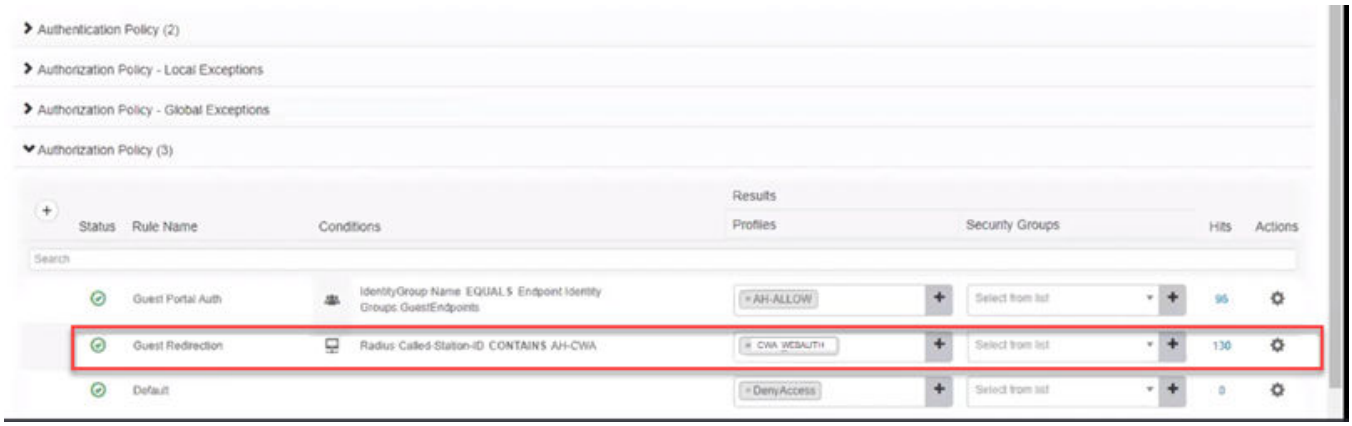


Figure 49: CWA Policy Set – Profile CWA_WebAuth

3. To view the Authorization Policy that was configured in Step 1, select Policy Set **AH-CWA**, and then select the **Authorization Policy** drop-down.
4. The Authorization Profile on the CWA server will return the role `ACL_WEBAUTH_Redirect` and the redirection URL.

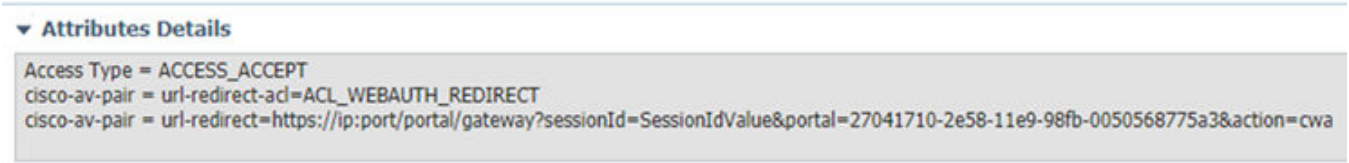


Figure 50: Attributes that the CWA server returns to ExtremeCloud IQ Controller

5. On the Cisco® ISE server, go to **Authorization** > **Authorization Profile**.
6. Create an allow Authorization Profile that is assigned to the user after the user is authenticated through the captive portal.

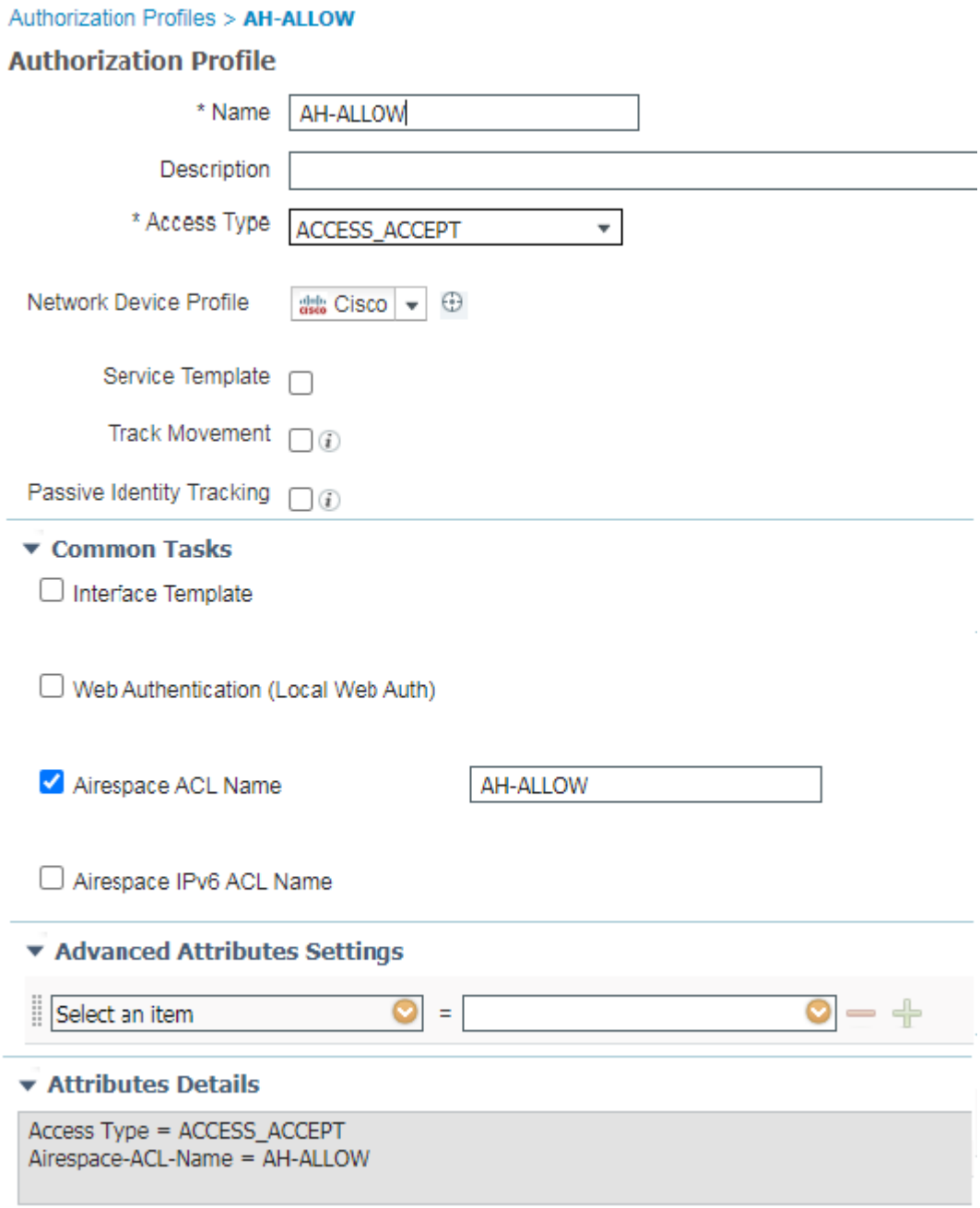


Figure 51: Allow Authorization Profile

- In the Common Tasks section, select **Airespace ACL Name**. The field must match the final Authenticated Role on ExtremeCloud IQ Controller.
- In the Attribute Details section, the Cisco® ISE server returns: `Access Type = ACCESS_ACCEPT`, and `Airespace-ACL-Name = x` where x is the name of the authenticated role on ExtremeCloud IQ Controller (AH-ALLOW).

7. On the Cisco® ISE server, go to **Policy** > **Policy Sets**, an open the policy set `AH-CWA` (described in Step 2).
8. Create an Authorization Policy that returns the Authorization Profile described in Step 6 with the following condition:

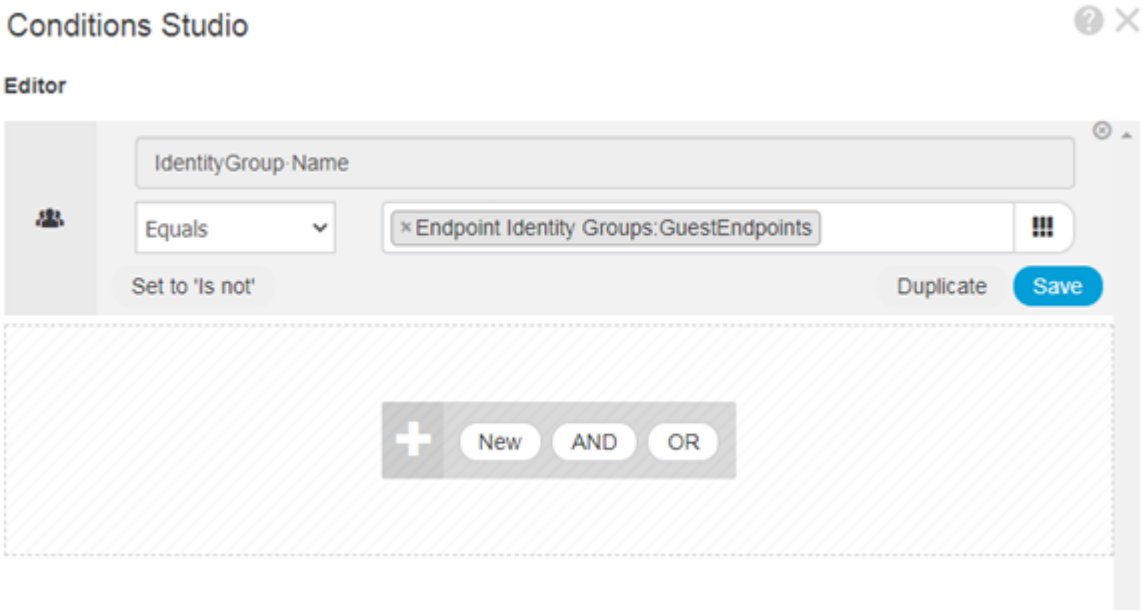


Figure 52: Allow Condition to match on Endpoint Identity

Note
Place this condition at the top of the conditions list.

CWA with ExtremeControl Deployment

This section outlines the configuration settings for Centralized Web Authentication (CWA) integration with ExtremeControl captive portal server.

Related Topics

Configure AAA Policy — ExtremeControl on page 145
CWA Network Settings - ExtremeControl on page 149
CWA Policy Redirection Role — ExtremeControl on page 152
CWA Server Configuration — ExtremeControl on page 154

Configure AAA Policy — ExtremeControl

You can create a AAA Policy that can be referenced through a WLAN Service, bypassing the local Network Access Control on ExtremeCloud IQ Controller.

Note
AAA Policy can only be configured for WLAN Networks requiring MACAUTH, External Captive Portal, or EAP.

To configure a AAA network policy:

1. Go to **Configure** > **Networks** > **WLANs** and select a network.

   AAA Policy is displayed for WLAN Networks that require authentication or authorization. The value **Local Onboarding** refers to RADIUS requests that are directed through the ExtremeCloud IQ Controller. Local Onboarding is the default value for WLAN Networks configured for Internal Captive Portal.
2. Select an **Auth Type**.

   The AAA Policy field displays.
3. From the AAA Policy field, select to add a new policy, or select to edit a policy.

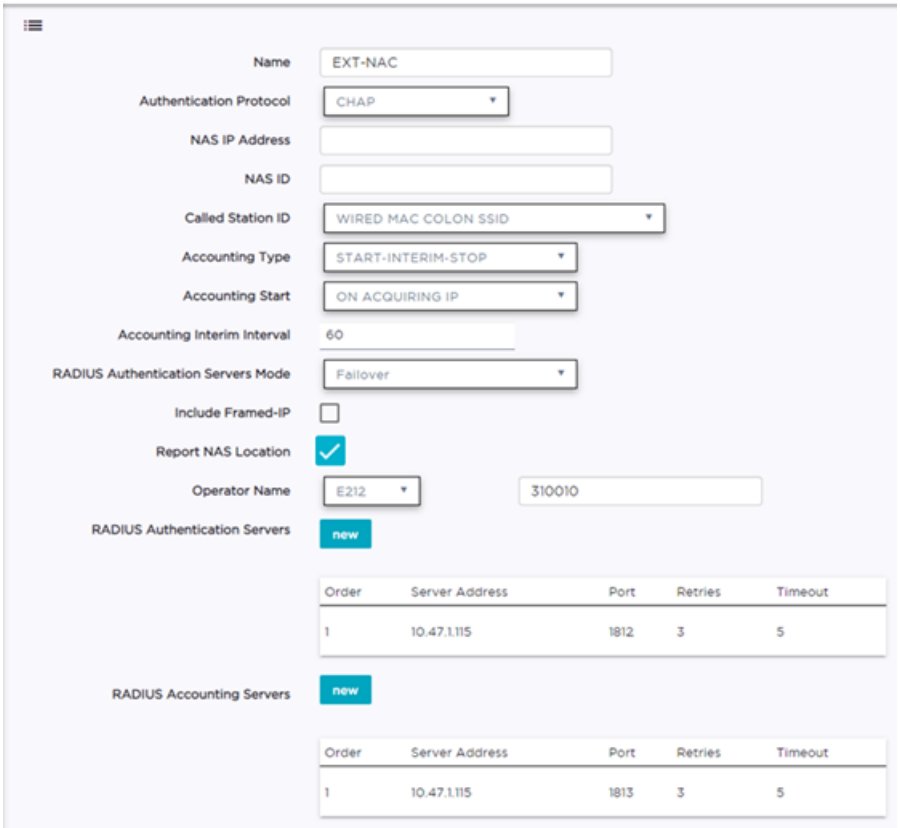


Figure 53: Centralized Web Authentication AAA Policy — ExtremeControl

4. Configure the following parameters:

   Name

   Policy name.

   Authentication Protocol

   Authentication protocol type for the RADIUS server (PAP, CHAP, MS-CHAP, or MSCHAP2).

   NAS IP Address

   IP address of the Network Access Server (NAS).

   NAS ID

A RADIUS attribute that identifies the client to a RADIUS server. The NAS-Identifier can be used instead of an IP address to identify the client.

Call Station ID

Identifies a group of access points. The Call Station ID is often configured in a large network using an external NAC or RADIUS server. Possible values are:

- Wired MAC: SSID
- BSSID (APs supported on a Centralized site only)
- Site Name
- Site Name: Device Group Name
- AP Serial Number

Note
Call Station ID allows for Zone authentication with a Centralized site.

- Site Campus
- Site Region
- Site City

Accounting Type

Determines when the appliance generates the accounting request. Valid values are:

- Start-Interim-Stop — Start record after successful login by the wireless device, interim record, and an accounting stop record based on session termination.
- Start-Stop — Start record after successful login by the wireless device user and an accounting stop record based on session termination.

The appliance sends the accounting requests to a remote RADIUS server.

Wait for client IP before starting accounting procedure

By default, the Accounting Start record is generated when the client is authenticated. Enable this setting to generate the Accounting Start record when the client acquires a non local IP address. Use this option for captive portals, which use RADIUS Accounting to learn of the client IP address before providing the landing page.

Accounting Interim Interval

The number of seconds (60-3600) between each interim update for a specific session. Default value is 60.

RADIUS Authentication Servers Mode

Select the availability behavior for RADIUS servers. Valid values are: **Failover** or **Load Balance**.

AAA Policy supports the ability to load balance RADIUS requests across target servers in a load-balancing pool. (A minimum of two servers is required.) Each client authentication session begins and ends on a single RADIUS server. The ExtremeCloud IQ Controller validates that each server can be reached and logs

an alert when a server in the pool is unreachable. The server pool is readjusted based on the status of each server in the pool.

Note
Configure one server for both Accounting and Authentication purposes.

When this setting is set to **Failover**, a RADIUS request is sent to one server at a time:

- The RADIUS request is sent to the Primary server (based on the RADIUS server order in the AAA policy).
- When the Primary server is not accessible, the request is sent to the second server (the Failover server).
- When the Primary server is accessible, the request is automatically sent to the Primary server instead of the Failover server.

Note
The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

When this setting is set to **Load Balance**, a RADIUS request is sent in round robin fashion:

- When a RADIUS server is not accessible, ExtremeCloud IQ Controller stops sending requests to that server.
- When a server is accessible, the server is added to the pool of servers.

Note
The RADIUS Status message (RFC 5997) indicates if the RADIUS server is accessible.

Include Framed IP

Select this option to include the FRAMED-IP attribute value pair in the RADIUS ACCESS-REQ message. You can include the user IP address in the RADIUS ACCESS-REQ through the FRAMED-IP attribute. This can extend user access reporting capabilities. Framed IP is supported by External Captive Portal only. Centralized Web Authentication does not support Framed IP.

Report NAS Location

Sends Network Access Server (NAS) Location per the RFC5580 Out of Band agreement. After a NAS Location change, the new NAS Location is reported in the next RADIUS Request or RADIUS Accounting message.

Note
Mid-session requests and the Initial Server Request for Location as described in RFC5580 are not supported.

The following additional attributes (AVP) used by RFC5580 are supported:

- LOCATION-INFO
- LOCATION-DATA

Note
Site Location details are reported in LOCATION-DATA. For more information on Site Location information, see the User Guide.

- BASIC-LOCATION-POLICY-RULES
- OPERATOR-NAME (Described below)

Operator Name

RADIUS attribute comprised of the operator namespace identifier and the operator name. The combination of operator name and namespace identifier uniquely identifies the owner of an access network. The Operator Name cannot exceed 253 bytes. Valid values are:

- Tadig — Three-character Country Code followed by a two- character alphanumeric operator ID
- Realm — Registered Domain Name of Operator
- E212 — Mobile Country Code or Mobile Network Code
- OneCC — Three-character Country Code followed by 1-6 uppercase ITU Carrier Codes
- None

RADIUS Authentication Servers

To add RADIUS servers for authentication, select **Add**. You can configure up to four RADIUS servers for authentication.

We have the CWA server configured.

RADIUS Accounting Servers

To add RADIUS servers for accounting, select **Add**. You can configure up to four RADIUS servers for accounting.

We have the CWA server configured.

Related Topics

RADIUS Settings on page 135
Centralized Web Authorization on page 127
CWA Network Settings - ExtremeControl on page 149
CWA Policy Redirection Role — ExtremeControl on page 152
CWA Server Configuration — ExtremeControl on page 154

CWA Network Settings - ExtremeControl

To configure a Centralized Web Authentication (CWA) captive portal:

1. Go to **Configure** > **Network** > **WLANS**.

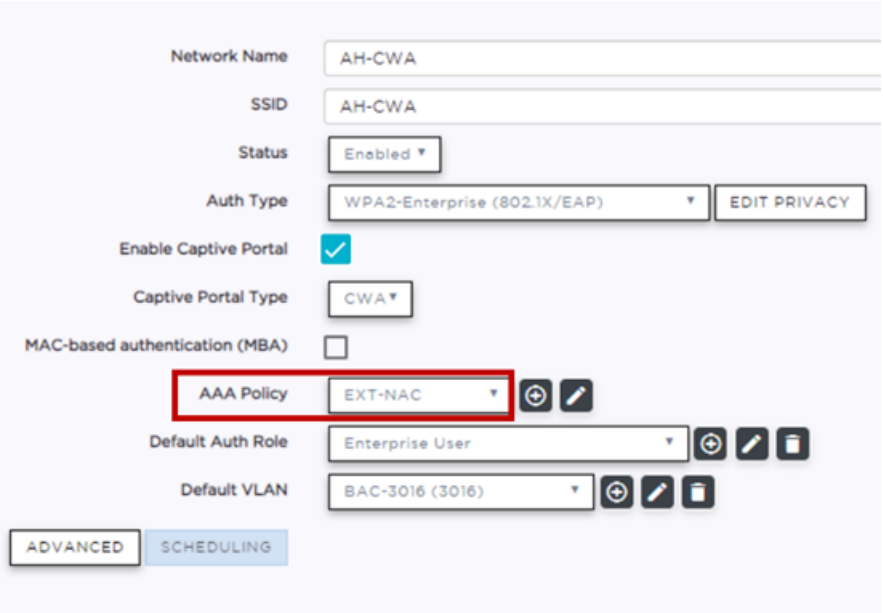


Figure 54: CWA Network on ExtremeCloud IQ Controller — ExtremeControl

2. Configure the following settings:

Table 20: Centralized Web Authentication Network Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Maximum 32 characters. Upper and lowercase allowed. Example: PermanentStaff
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.
Auth Type	The Authorization Type for a CWA captive portal must be **WPA2 Enterprise (802.1x EAP)**
Enable Captive Portal	Select this option to configure a captive portal network.

Table 20: Centralized Web Authentication Network Settings (continued)

Field	Description
MAC-Based Authentication	(Optional) Select this option to enable MBA. When selected, multi-factor authentication is enabled. The following parameter displays when MAC-based Authentication is enabled: • **MBA Timeout Role**. Select the role that will be assigned to a wireless client during MAC-based authentication (MBA) if the RADIUS server access request times out. If no MBA Timeout Role is selected, then a RADIUS server timeout is treated like an Access-Reject, which prevents the client from accessing the network. Other options: ◦ — create a new role ◦ — edit role ◦ — delete role
Captive Portal Type	**CWA**
AAA Policy	Specify the AAA Policy associated with the captive portal. Define the RADIUS server used for authentication in the AAA Policy. This is the IP address of the captive portal on ExtremeControl. **Note:** Local Network Access Control is not supported.
Default Auth Role	Specify the default authorization role that is configured on ExtremeCloud IQ Controller.
Default VLAN	Specify the default VLAN that is configured on ExtremeCloud IQ Controller Bridged at AC VLANs are supported.

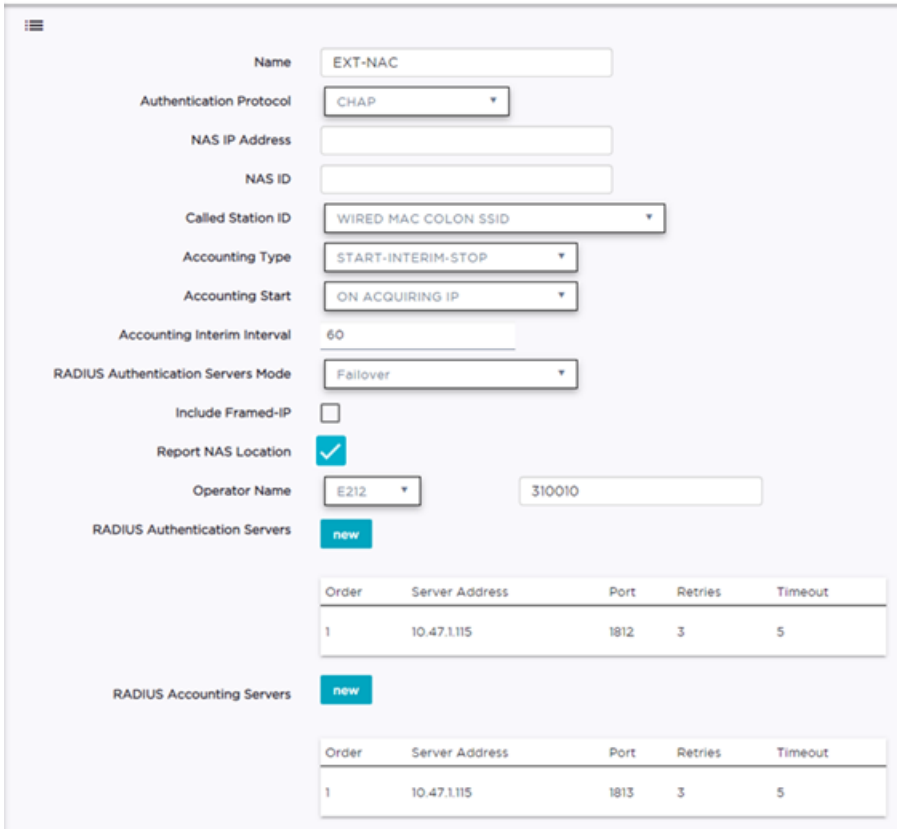


Figure 55: AAA Policy for CWA — RADIUS Server definition

For more information about creating policy roles or configuring VLANs, see the *ExtremeCloud IQ Controller User Guide*.

Related Topics

Centralized Web Authorization on page 127
Configure AAA Policy — ExtremeControl on page 145
CWA Policy Redirection Role — ExtremeControl on page 152
CWA Server Configuration — ExtremeControl on page 154

CWA Policy Redirection Role — ExtremeControl

To configure a policy role with at least one redirection rule:

1. Go to **Configure** > **Policy** > **Role** > **Add**.
2. Create a new role.
   - NAC_WEBAUTH_REDIRECT is the example redirection role for the ExtremeControl captive portal server.
3. Select **Layer 3/Layer 4** and configure the parameters for a redirect rule that works with CWA captive portal. See Table 21 on page 153.

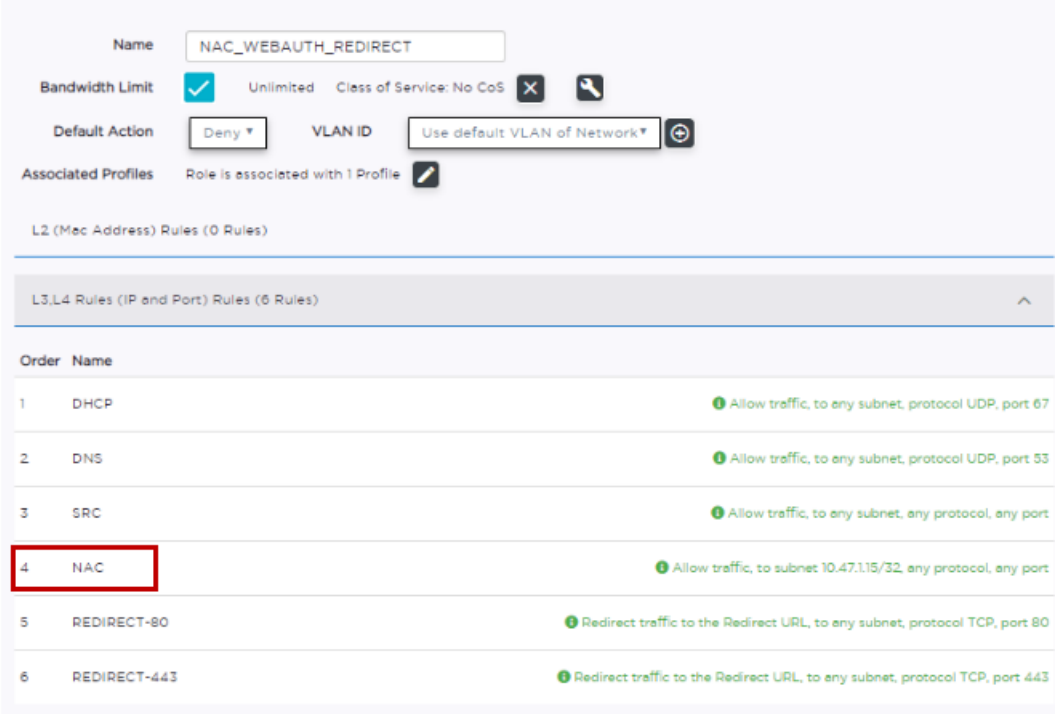


Figure 56: Example Redirection Role on ExtremeCloud IQ Controller that includes six L3/L4 rules

Figure 57: Redirect-80 rule redirects HTTP traffic from Port 80

Table 21: Rule Configuration for Layer3/Layer4 Redirection Rules

Field	Description
Name	Provide a name for the rule. Example: **Redirect-80** that redirects traffic on HTTP port 80.
Action	**Redirect**
Protocol	**TCP**
IP/Subnet	**User-Defined**. Then specify the IP address of the captive portal. The redirection role includes a rule that points to the CWA server IP address.
Port	Include at least one rule for HTTP port 80 or HTTPS port 443 The redirection role includes a rule for both HTTP port 80 and HTTPS port 443

For more information about creating policy roles, see the *ExtremeCloud IQ Controller User Guide*.

Related Topics

Centralized Web Authorization on page 127

Configure AAA Policy — ExtremeControl on page 145
CWA Network Settings - ExtremeControl on page 149
CWA Policy Redirection Role — ExtremeControl on page 152
CWA Server Configuration — ExtremeControl on page 154

CWA Server Configuration — ExtremeControl

Configure an Authorization Policy on the CWA server to integrate with ExtremeCloud IQ Controller. From the CWA server, you configure the redirect policy to return the specific redirect rule that you configured on ExtremeCloud IQ Controller. The CWA Authorization Policy on the CWA server includes three profiles: the Redirection Profile that is referenced from ExtremeCloud IQ Controller, an Allow Profile, and a Deny Profile.

CWA integrates with a captive portal on an ExtremeControl server. The following topics outline how to configure the ExtremeControl captive portal server:

- Configure CWA on ExtremeControl on page 154

Related Topics

Centralized Web Authorization on page 127
Configure AAA Policy — ExtremeControl on page 145
CWA Network Settings - ExtremeControl on page 149
CWA Policy Redirection Role — ExtremeControl on page 152

Configure CWA on ExtremeControl

Configure CWA to integrate with an ExtremeControl server.

1. On the ExtremeControl server, create a policy mapping for the ExtremeCloud IQ Controller network:
   - Map the policy to the ExtremeCloud IQ Controller network name.
   - Provide the redirection rule that you created on ExtremeCloud IQ Controller as the Filter ID value.
   - Provide the Redirection URL as the Cisco RADIUS attribute value pair (AVP). For example: `cisco-avpair=url-redirect=http://10.47.1.15:80/`

   Note
   Do not include query parameters in the url-redirect. The following AVP is not valid: cisco-avpair=url-redirect=http://10.47.1.15:80/**?a=123**, where **?a=123** is a query parameter.

2. From the ExtremeControl server, go to **Configuration** > **Profiles** > **Policy Mapping**.

   The rules engine assigns the policy **Unregistered** to the redirection and assigns the policy **Enterprise User** when authenticated by the captive portal.

3. Create a new mapping for the **Unregistered** policy.

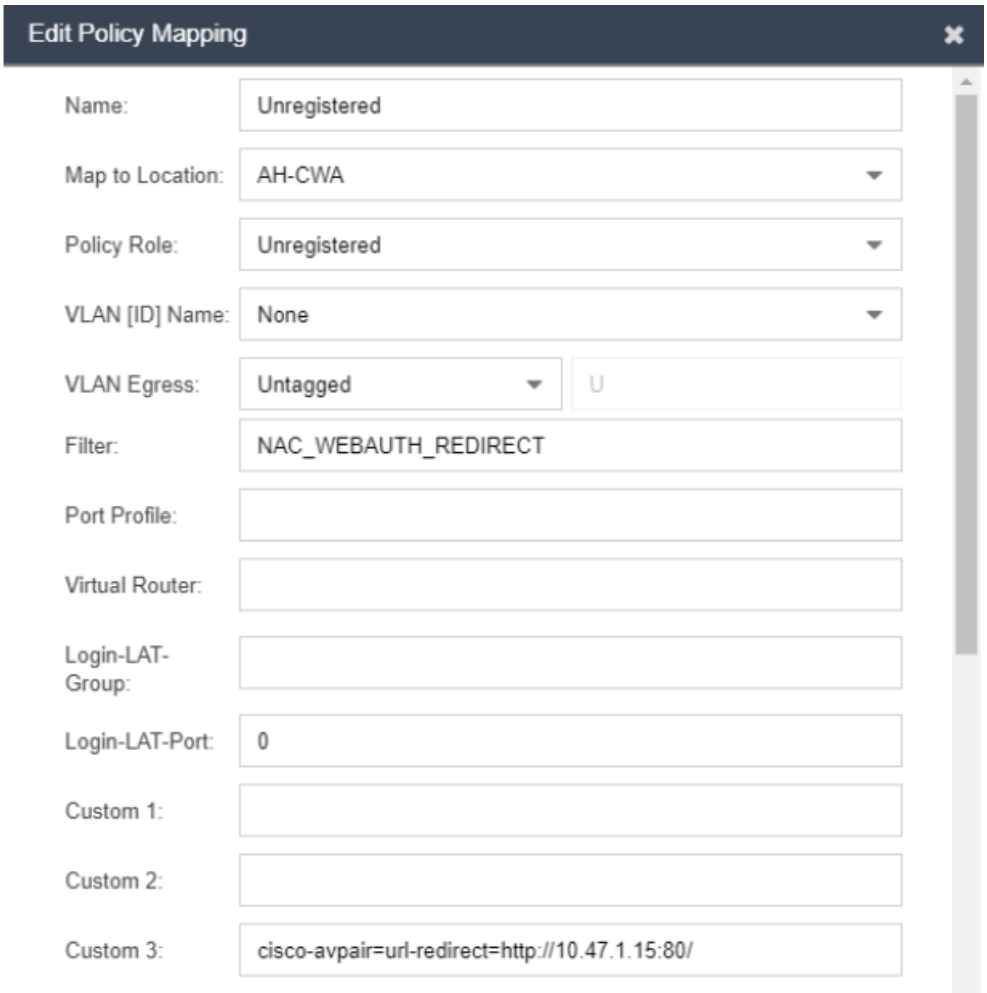


Figure 58: Redirect Policy Mapping on ExtremeControl — Unregistered Policy

- Location — Specify the CWA network name that you configured in ExtremeCloud IQ Controller.
- Filter — Specify the redirection rule that you configured on ExtremeCloud IQ Controller.
- Custom — Specify the AVP: `cisco-avpair=url-redirect=http://10.47.1.15:80/`

Verify the attributes specified by Filter and Custom 3 by editing the switch profile that corresponds to ExtremeCloud IQ Controller.

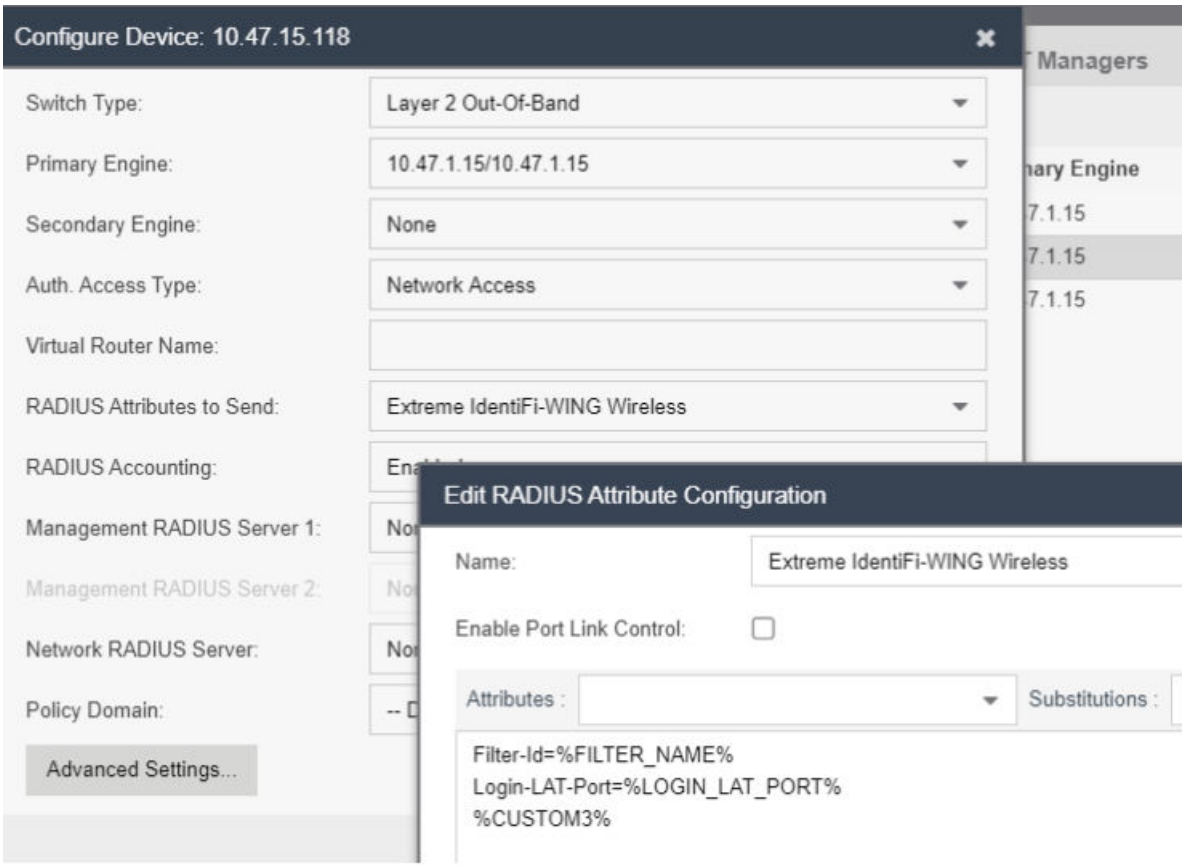


Figure 59: Switch RADIUS Attribute Configuration — Advanced Settings

4. Create a policy mapping for **Enterprise User**.

   You can use the default ExtremeCloud IQ Controller allow roles. For example the default Enterprise User, or you can configure your own role. Here our configured Enterprise User role includes the `AH-Allow` rule. Map the Enterprise User role to ExtremeControl.

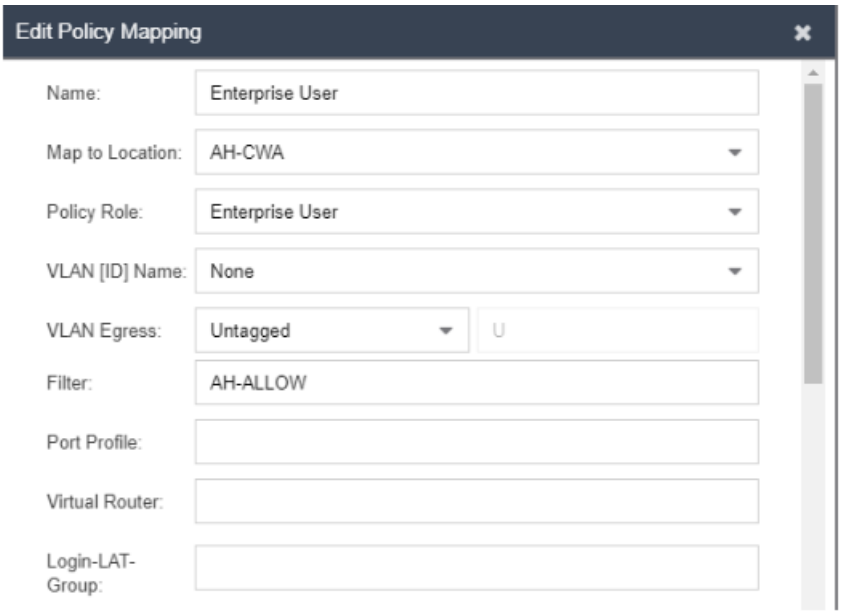


Figure 60: Allow Policy Mapping on ExtremeControl — Enterprise User

- Location — Specify the CWA network name that you configured in ExtremeCloud IQ Controller.
- Filter — Specify the allow policy rule that you configured on ExtremeCloud IQ Controller.

5. Assign both the allow policy role and the redirect policy role to the site configuration Profile on ExtremeCloud IQ Controller.
   a. Go to **Sites** and select the site.
   b. Select **Device Groups** and select the device group.
   c. Select **Profile** and edit the configuration Profile.
   d. Select **Roles** and select the following roles:
      - NAC_WEBAUTH-REDIRECT
      - Enterprise User

NAI Routing and Dynamic Discovery

AAA Policy Settings for NAI Routing on page 158
Configure a Regular Expression Realm on page 161

NAI (Network Access Identifier) routing allows for routing authentication requests to authentication servers based on the domain of the authenticated user. NAI Routing associates defined RADIUS servers with realms that match the user's domain name. You have the option to configure the RADIUS servers within the realm definition or you can configure the server to be discovered dynamically (RFC 7585). This is supported only for RADSEC enabled servers.

When **NAI Routing** is enabled, the **RADIUS Accounting Server Mode** setting on the AAA Policy is not displayed. ExtremeCloud IQ Controller selects the first functioning accounting server that is defined in the realm, similar to a Failover mode process. If the **Peer Discovery** setting is selected for RADIUS Accounting, then ExtremeCloud IQ Controller uses the discovered server for both authentication and accounting.

WBA OpenRoaming uses NAI Routing in the AAA policy that is automatically created with the OpenRoaming profile. You can also manually configure a AAA policy to support multiple realms on one AP radio. For more information on configuring Hotspot WBA OpenRoaming, see the ExtremeCloud IQ Controller User Guide.

Note
Existing AAA policies cannot be modified to enable NAI Routing. You must create a new AAA policy.

Related Topics

AAA Policy Settings for NAI Routing on page 158

AAA Policy Settings for NAI Routing

Details about specific AAA Policy settings that are used for NAI Routing:

Name

Policy name.

NAI Routing

Enable static Network Access Identifier (NAI) routing. Allows for an NAI Realm configuration.

> **Note**
> NAI Routing cannot be enabled for a Local Onboarding AAA Policy, and only RADSEC enabled servers can be associated with realms.

Authentication Protocol

Authentication protocol type for the RADIUS server (PAP, CHAP, MS-CHAP, or MSCHAP2).

Call Station ID

Identifies a group of access points. The Call Station ID is often configured in a large network using an external NAC or RADIUS server. Possible values are:

- Wired MAC: SSID
- BSSID (APs supported on a Centralized site only)
- Site Name
- Site Name: Device Group Name
- AP Serial Number

> **Note**
> **Call Station ID** allows for Zone authentication with a Centralized site.
> - Site Campus
> - Site Region
> - Site City

Accounting Type

Determines when the appliance generates the accounting request. Valid values are:

- Start-Interim-Stop — Start record after successful login by the wireless device, interim record, and an accounting stop record based on session termination.
- Start-Stop — Start record after successful login by the wireless device user and an accounting stop record based on session termination.

The appliance sends the accounting requests to a remote RADIUS server.

Wait for client IP before starting accounting procedure

By default, the Accounting Start record is generated when the client is authenticated. Enable this setting to generate the Accounting Start record when the client acquires a non local IP address. Use this option for captive portals, which use RADIUS Accounting to learn of the client IP address before providing the landing page.

Accounting Interim Interval

The number of seconds (60-3600) between each interim update for a specific session. Default value is 60.

Operator Name

RADIUS attribute composed of the operator namespace identifier and the operator name. The combination of operator name and namespace identifier uniquely identifies the owner of an access network. The Operator Name cannot exceed 253 bytes. Valid values are:

- None
- Tadig — Three-character Country Code followed by a two- character alphanumeric operator ID
- Realm — Registered Domain Name of Operator
- E212 — Mobile Country Code or Mobile Network Code
- OneCC — Three-character Country Code followed by 1-6 uppercase ITU Carrier Codes
- WBAID — Used with a WBA OpenRoaming AAA policy that is automatically generated when using an OpenRoaming Hotspot. For more information on Hotspot, see the ExtremeCloud IQ Controller User Guide.

Realm Entries

Note
Realm entries are available when **NAI Routing** is selected. Up to four realm entries are supported per AAA policy and each realm supports four Authentication servers and four Accounting servers.

To add a new realm entry:

1. Select **New** and provide an **NAI Realm** value.

   Configure the Realm Name in accordance with the user domain name.
2. Select **New** to add RADIUS server settings for Authentication and Accounting servers respectively.

Use the NAI Routing in the RADIUS packet to dynamically discover the RADIUS server for the realm. Enter an asterisk (*) as the realm name and enable **Peer Discovery** in the RADIUS Settings on page 135. Dynamic Discovery eliminates the need for static configuration of the server IP address.

When the realm name specifies an asterisk, it matches any realm specified in the Username attribute. If the realm specifies a string, matching looks for an @ in the Username RADIUS attribute and performs an exact, case insensitive match between what comes after the @ and the name of the realm. For example, if the received Username RADIUS attribute is `anonymous@example.com`, then the lookup is for `example.com`. If the realm name starts with a /, the name is treated as a regular expression. A case insensitive regular expression match is performed using the regular expression on the value of the entire Username attribute. A trailing / indicates the end of the regular expression. A trailing / is optional.

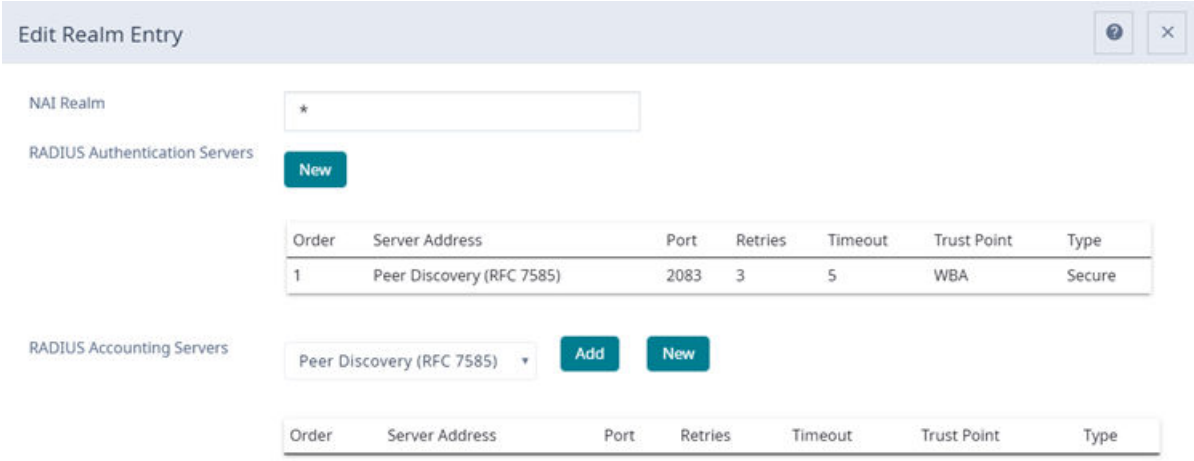


Figure 61: Realm Configured for Dynamic Discovery

Related Topics

Configure a Regular Expression Realm on page 161
RADIUS Settings on page 135

Configure a Regular Expression Realm

It is possible to create realms in NAI Routing based on a regular expression. When the realm name starts with a `/`, the name is treated as an regular expression and the value of the entire Username attribute is matched. Optionally, you can end the regular expression with a trailing `/`.

For example, to match on the domain name `example.com`, configure a realm block named `/@example\.com$/`, and to match all domains under the .com top domain, configure the following name `/@.*\.com$/`.

Because the matching is done on the entire attribute value, you can use rules to load balance users in a specific domain. For example, the following realm name directs some users to match on one realm block configured for one server, while other users will match another realm block configured for another server:

```
/^[a-k].*@example\.com$/
```

Figure 62 illustrates a realm configuration that uses a regular expression to load balance traffic based on device MAC address. Devices with a MAC address that start with `88` are sent to IP address `10.47.15.21`, while devices with a MAC address that start with `44` are sent to IP address `10.47.15.23`.

Realm Entries New

Order	Realm	Trust Point	Type	AAA Auth/Acct	Server Address
1	/^88/	H1	Secure	Authentication	10.47.15.21
2	/^44/	H3	Secure	Authentication	10.47.15.23

Figure 62: Regular Expression Realm Configuration

Related Topics

AAA Policy Settings for NAI Routing on page 158

Deploying ExtremeCloud IQ-SE as an External Captive Portal

Configuring an External Captive Portal Network on page 164
Editing the Configuration Profile for Network and Roles on page 168
ExtremeCloud IQ Controller Default Pass-Through Rule on page 168
Adding ExtremeCloud IQ Controller as a Switch to ExtremeCloud IQ - Site Engine on page 170
Editing the Unregistered Policy on ExtremeCloud IQ - Site Engine on page 175
Editing the ExtremeCloud IQ - Site Engine Profile for Policy and Location-Based Services on page 177

Deployment Strategy

The following strategy outlines how to configure ExtremeCloud IQ Controller to integrate with ExtremeCloud IQ - Site Engine (XMC), which houses the external captive portal, handling client authentication. The portal resides on the ExtremeControl engine and ExtremeCloud IQ Controller handles the client network connections. Traffic connecting to the Guest network will send and receive all RADIUS requests from the externally defined RADIUS server, not from the ExtremeCloud IQ Controller that processes the request. The ExtremeControl engine provides RADIUS authentication and authorization and policies that are defined in ExtremeCloud IQ - Site Engine.

The following outlines how to integrate ExtremeCloud IQ Controller with ExtremeCloud IQ - Site Engine, configuring an External Captive Portal on the ExtremeControl engine.

1. If you are authentication with Local Onboarding, create a RADIUS pass-through rule on ExtremeCloud IQ Controller.

   Note
   It is possible to authenticate directly to the AAA RADIUS server. Refer to the ExtremeCloud IQ Controller User Guide for information about AAA RADIUS Authentication.

2. Add ExtremeCloud IQ Controller to ExtremeCloud IQ - Site Engine as a switch.

3. On ExtremeControl, create an Unregistered Policy for the ExtremeCloud IQ Controller Pass-Through Network.
4. Edit the ExtremeControl configuration profile, associating network policy and Location-Based Services.

Configuring an External Captive Portal Network

Configuring an External Captive Portal network.

1. Go to **Configure** > **Networks** > **WLANs** > **Add** and configure the following parameters:

   Network Name

   Guest

   SSID

   Guest

   Auth Type

   Open

   Enable Captive Portal

   Check this option and specify the following parameters:

   Captive Portal Type

   External

   ECP URL

   (http/https)://nac1.extremenetworks.com

   FQDN should be resolvable by connecting end systems via DNS.

   Note
   Walled Garden rules are not required for this network. The process of enabling a captive portal on the network automatically creates rules allowing DNS, DHCP, and redirection rules. However, if users are unable to connect to the network, consider creating specific DNS and DHCP Allow rules as a Walled Garden configuration.

   When you enable Captive Portal on a WLAN ExtremeCloud IQ Controller automatically builds the role and redirect rules required for captive portal based on the Network Name configured in the WLAN.

   Identity/ Shared Secret

   Not required with integration with Extreme Control.

   Used when building a back-end captive portal server to integrate with the system. ExtremeCloud IQ Controller sends the Identity/Shared Secret and receives a response token.

   Use HTTPS

   Select this option if you want ExtremeCloud IQ Controller to attempt to redirect SSL traffic.

Best Practice: Use https:// in the ECP URL and de-select this option.

Send Successful Login To

Original Destination. Or, enter the redirection URL here.

MAC-based authentication (MBA)

Enable and configure the following parameters:

MBA Timeout Role

Enterprise User

AAA Policy

Local Onboarding

Traffic passes through the internal Network Access Control engine, which is configured to proxy traffic to the ExtremeCloud IQ - Site Engine server control engines.

Note
It is possible to authenticate directly to the AAA RADIUS server. Refer to the ExtremeCloud IQ Controller User Guide for information about AAA RADIUS Authentication.

Authentication Method

Proxy RADIUS

Primary RADIUS

IP address of the Access Control Engine.

Configure a primary and backup if you have more than one Access Control Engine.

Authenticate Locally for MAC

Must be *Disabled* for external captive portal on the NAC server.

Default Auth Role

Enterprise User

Default VLAN

Bridged at AP Untagged

2. Select **Advanced** and configure the following parameters:

RADIUS Accounting

Enabled

Pre-authenticated idle timeout

Default value: 300 seconds

Post-authenticated idle timeout

Default value: 1800 seconds

Maximum session timeout

Default value: 0 seconds

End-systems are re-authenticated on ExtremeCloud IQ Controller, not from the ExtremeCloud IQ - Site Engine Access Control Engine. Therefore, ExtremeCloud IQ Controller ignores ExtremeCloud IQ - Site Engine re-authentication requests to modify filter-ids (policies). Modification of these timeout values initiates re-authentication from the ExtremeCloud IQ Controller to the ExtremeCloud IQ - Site Engine Access Control Engine, resulting in modification of the policy/filter-id as expected.

Note
There may be a delay or network interruption on policy changes. Adjust the timeout values if you do not see a timely policy change or if you experience network interruptions during the connection attempts from clients.

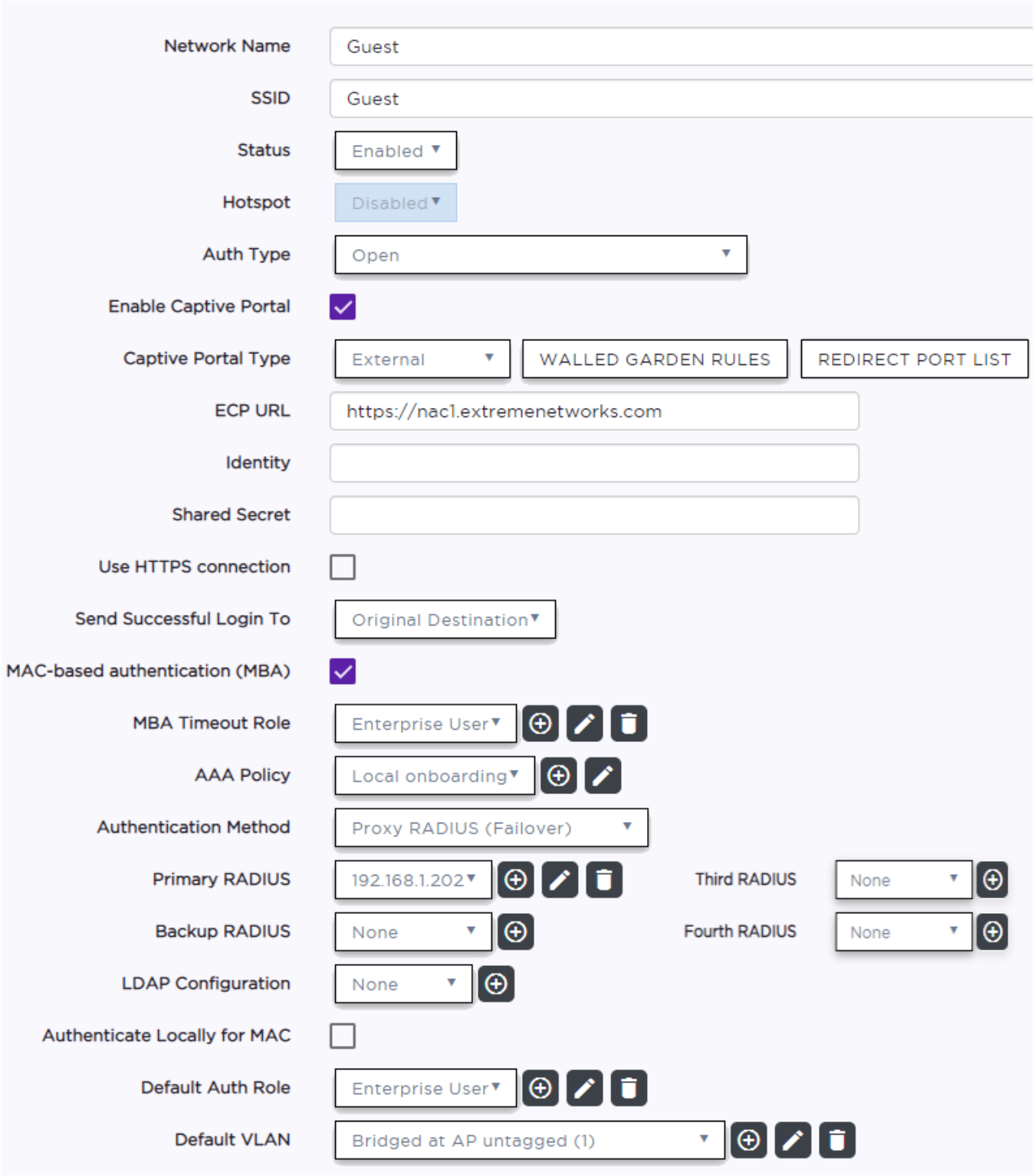


Figure 63: Network Settings ExtremeCloud IQ Controller

3. Select **Save** to save the WLANS settings.

   You can assign the Network to device group configuration Profiles now or later.

4. Select **Yes** to assign the WLAN to desired device groups or **SKIP** to assign them later.

Editing the Configuration Profile for Network and Roles

Configure a network and be aware of policy roles that you are using before modifying the device group profile.

1. On ExtremeCloud IQ Controller, go to **Configure** > **Sites** and select a site.
2. Select **Device Groups** tab.
3. Select your configured device group.
4. Beside the Profile field, select ✎ to edit the configuration profile.
5. From the **Networks** tab, assign a radio to the network you created.
6. From the **Roles** tab, select the appropriate roles that will be applied to the end system during connection/registration/authorization. Typically all roles are selected.

   Note
   Upon creating an External Captive Portal WLAN the ExtremeCloud IQ Controller automatically creates the following internal rule:

   - Unregistered role for <network name>

   ```
   The following are rule examples:
   Unregistered role for Guest:acfilters# show
   Custom AP Filters: disable
   filter 1 3 proto udp eth 800 mac any 0.0.0.0/0 port 53 in dst out src allow
   filter 2 3 proto udp eth 800 mac any 0.0.0.0/0 port 67 in dst out src allow
   filter 3 3 proto any eth any mac any 0.0.0.0/0 all_ports in none out src allow
   filter 4 3 proto icmp eth 800 mac any 0.0.0.0/0 type-code 0x0000 0x0000 in
   dst out src allow
   filter 5 3 proto tcp eth 800 mac any 1.1.1.1/32 all_ports in dst out src allow
   filter 6 3 app-signature group "Web Applications" hostname
   "fqdn:nac_engine.mynetwork.com" proto any eth 800 mac any 0.0.0.0/0 all_ports
   in dst out src allow
   filter 7 3 proto tcp eth 800 mac any 0.0.0.0/0 port 80 in dst out none
   redirect
   filter 8 3 proto tcp eth 800 mac any 0.0.0.0/0 port 443 in dst out none
   redirect
   ```

   Enabling Captive Portal on a WLAN automatically builds the Unregistered role for <Network Name> and the necessary rules for client redirection. This role is automatically assigned to device groups that have the External Captive Portal WLAN selected to broadcast. Unregistered role for <Network Name> is not visible within the ExtremeCloud IQ Controller user interface. No modification or role creation is necessary for the functional External Captive Portal environment. Extreme Control *must* send back the filter-id of Unregistered role for <Network Name> to use the automatically created role.

7. Select **Save** to save the Profile settings.
8. Select **Close** to close the device group.

ExtremeCloud IQ Controller Default Pass-Through Rule

Create a RADIUS Pass-Through rule on ExtremeCloud IQ Controller. This rule designates that traffic connecting to the Guest network will send and receive

all RADIUS requests from the externally defined RADIUS server, not from the ExtremeCloud IQ Controller that processes the request. This includes filter-ids that are received as attributes. The ExtremeControl RADIUS server provides RADIUS authentication and authorization and policies that are defined in ExtremeCloud IQ - Site Engine.

1. On ExtremeCloud IQ Controller, go to **Onboard** > **Rules** > **Add**.
2. Configure the following parameters:

   Name

   Guest

   Rule Enabled

   Select this option to enable the new rule.

   Location

   SSID: Guest

   Accept Policy

   Pass-Thru External RADIUS
3. Select **Save**.
4. Move the rule to the top of the rule set, if it is not already there.

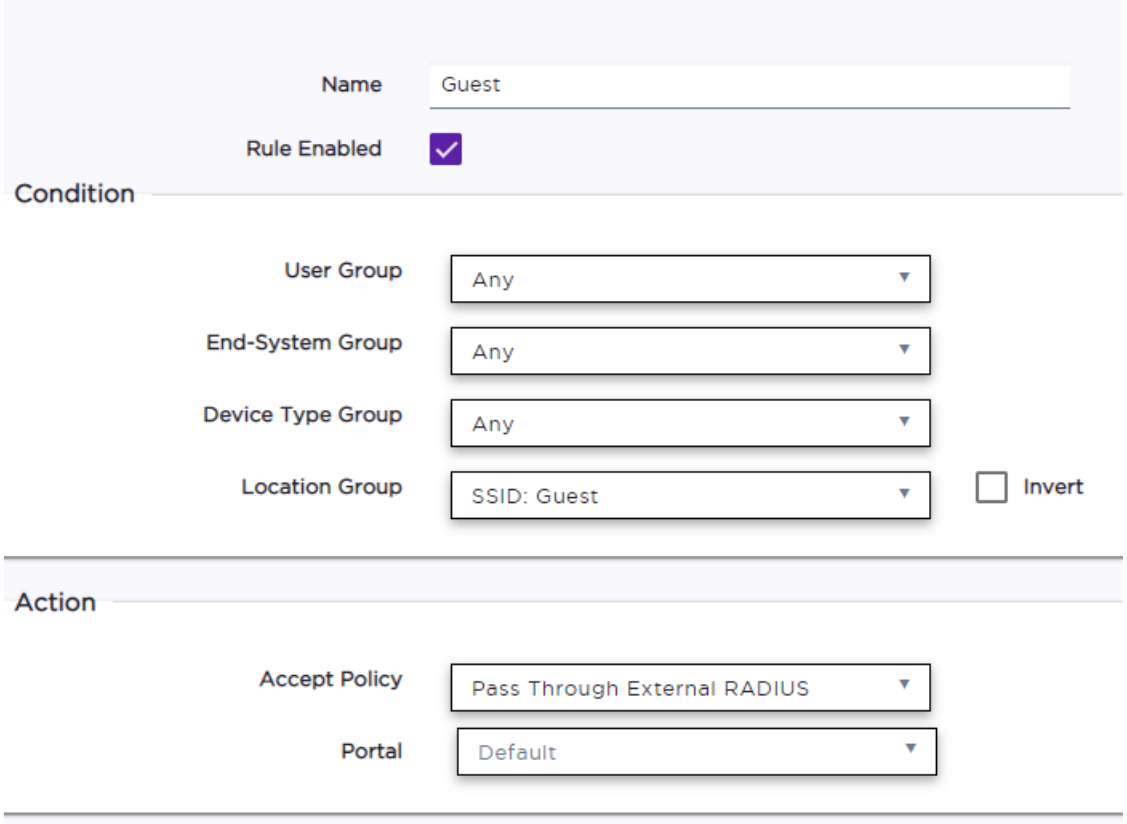


Figure 64: Guest Rule ExtremeCloud IQ Controller

Adding ExtremeCloud IQ Controller as a Switch to ExtremeCloud IQ - Site Engine

1. From ExtremeCloud IQ - Site Engine, add a device profile for ExtremeCloud IQ Controller.
   a. To open the **Add Profile** window, go to **Administration** > **Profiles** > **Add**.
   b. Provide the **Profile Name** and **SNMP Version** and settings.
2. Select the **CLI Credentials** field and configure the CLI credentials.

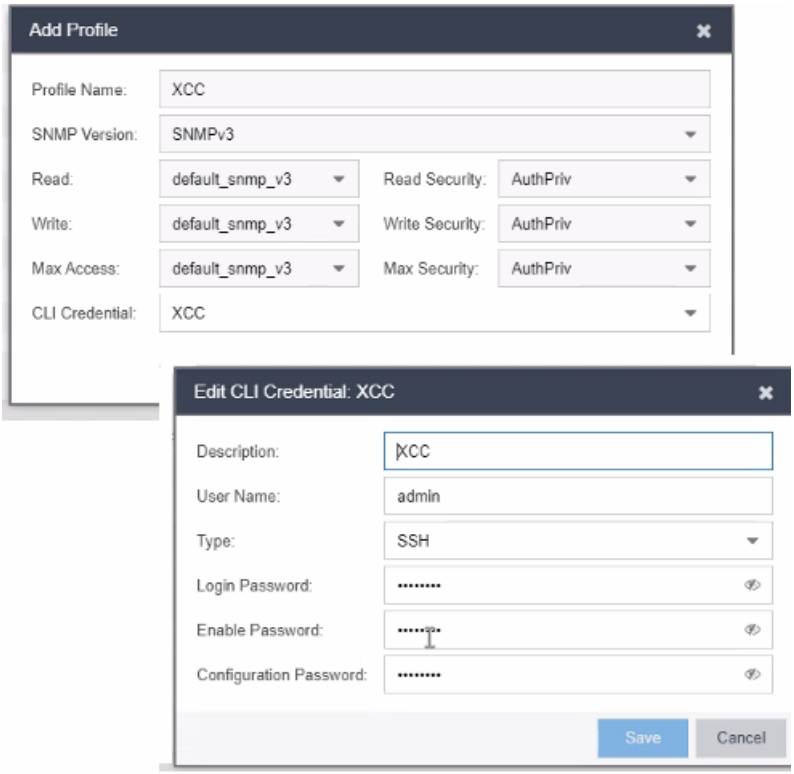


Figure 65: Adding an Extreme Management Center Profile

> **Note**
> You must add the ExtremeCloud IQ Controller password three times. Add the same password to the following fields:
> - Login Password
> - Enable Password
> - Configuration Password

3. Add the switch to **Network Devices**.
   a. Select **Network** > **Devices**.
   b. Right click **World** or the appropriate site object.

c. Select **Add Device**

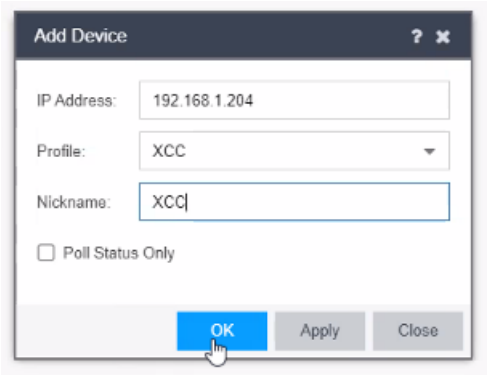


Figure 66: Add ExtremeCloud IQ Controller as a device in ExtremeCloud IQ - Site Engine

a. Enter The IP address of ExtremeCloud IQ Controller.
b. Select the profile that you created.
c. Select **OK**.

4. Add the switch to your **Access Control Engine**.
   a. Select **Control** > **Access Control** > **Engines**. From the All Engines panel, select the Engine.
   b. Select **Switches** > **Add**.
   c. From the **Devices** tree, select the newly added device.

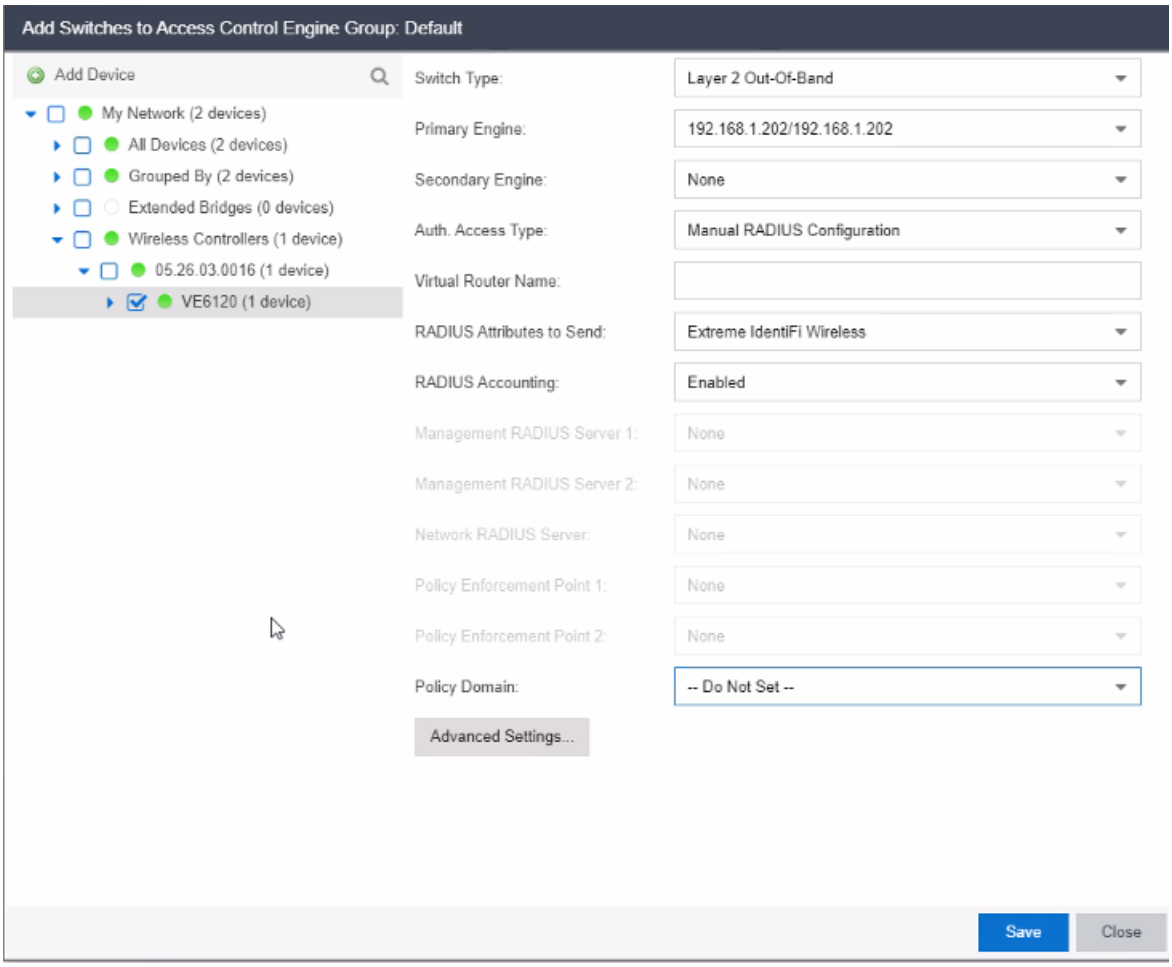


Figure 67: Add Switch - ExtremeCloud IQ Controller

5. Configure ExtremeCloud IQ Controller switch attributes:
   - Switch Type: **Layer 2 Out-Of-Band**
   - Primary Engine: Select the Access Control Engine that you set as the RADIUS server for the network on the ExtremeCloud IQ Controller.
   - Secondary Engine (if appropriate for your configuration)
   - Edit Auth Access Type: **Manual RADIUS Configuration**
   - Select the drop-down for **RADIUS Attributes to Send** and select **New**.
   - Insert the following into the new attributes schema:

```
Filter-Id=%POLICY_NAME%
Login-LAT-Port=%LOGIN_LAT_PORT%
Service-Type=%MGMT_SERV_TYPE%
```

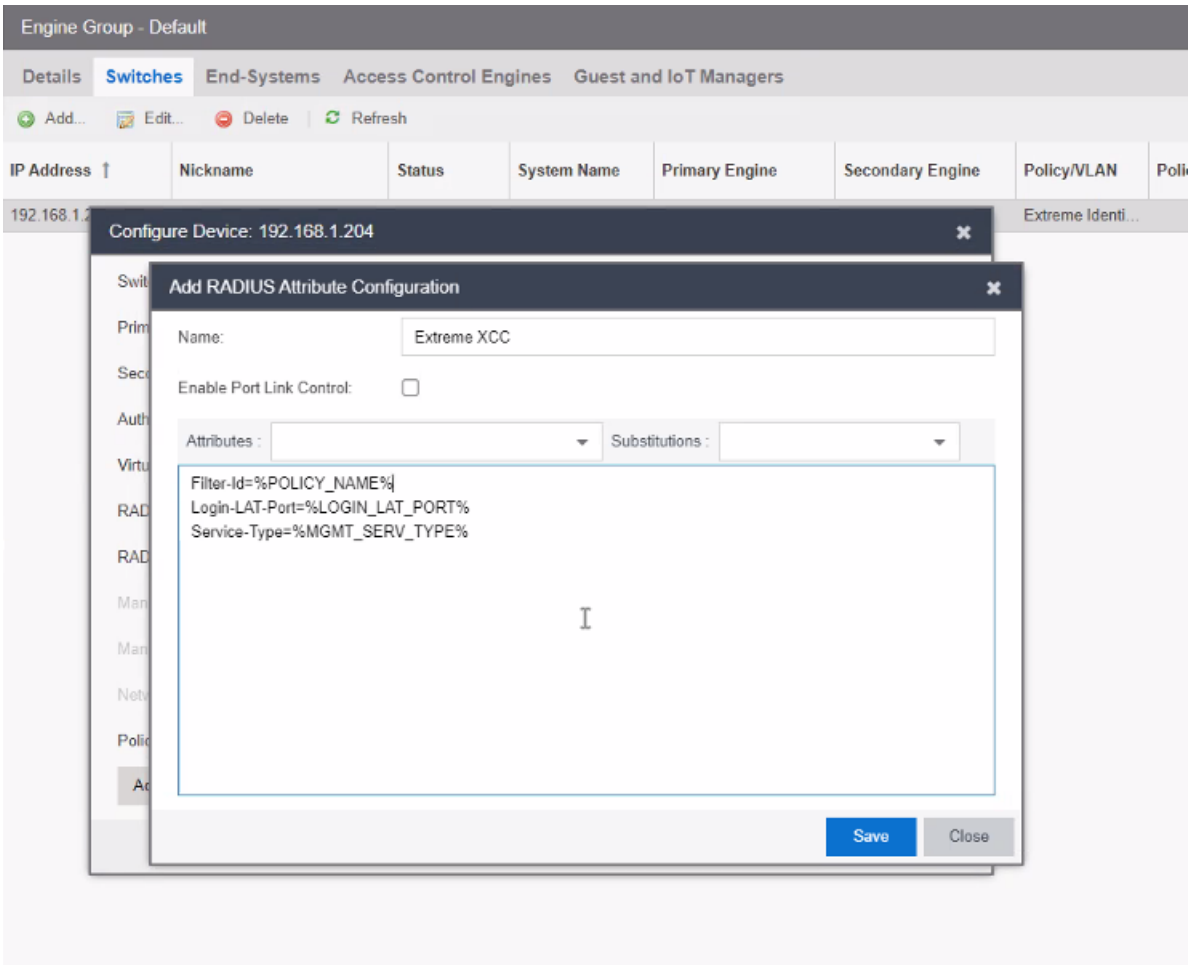


Figure 68: New RADIUS Attribute for ExtremeCloud IQ Controller

6. Save the new attribute Schema as **RADIUS attribute to send**.

7. Set RADIUS accounting to **Enabled**.

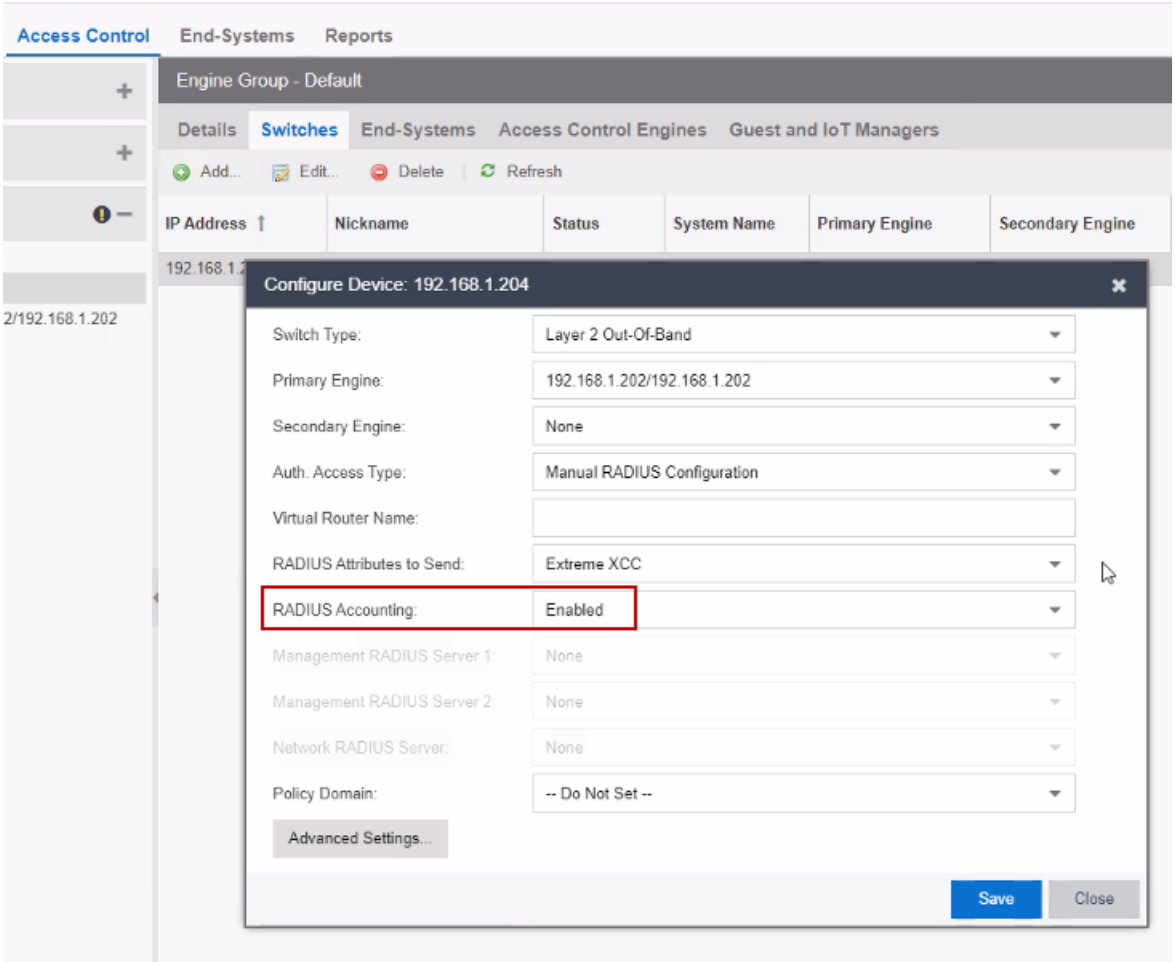


Figure 69: ExtremeCloud IQ Controller Switch Device Settings

8. Select **Save**.

9. Enforce the changes.

   From the Engine Groups, right-click the IP address of ExtremeCloud IQ Controller. Then, select **Enforce**.

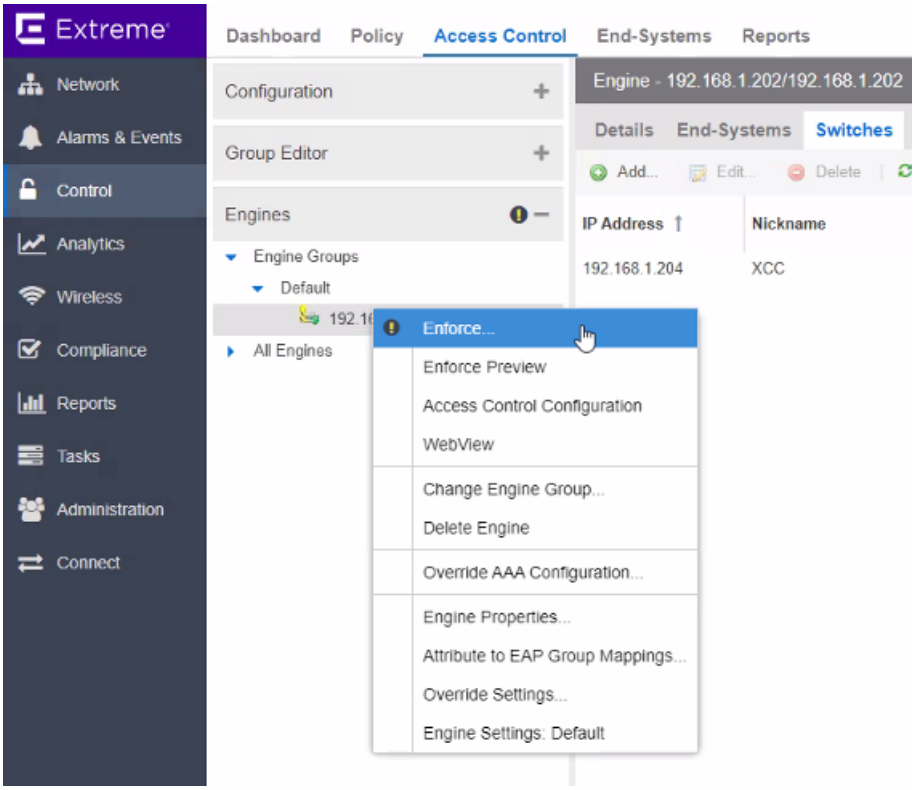


Figure 70: Enforce Changes

Editing the Unregistered Policy on ExtremeCloud IQ - Site Engine

Edit the default ExtremeCloud IQ - Site Engine Unregistered policy to work with ExtremeCloud IQ Controller. The Unregistered role on ExtremeCloud IQ Controller is specifically *Unregistered role for <Network Name>*, where *<Network Name>* is the Network Name configured in the WLAN on the ExtremeCloud IQ Controller.

1. In ExtremeCloud IQ - Site Engine, edit the Policy mapping to specify *Unregistered role for <NETWORK NAME>*. In this example, <NETWORK NAME> is **Guest**.

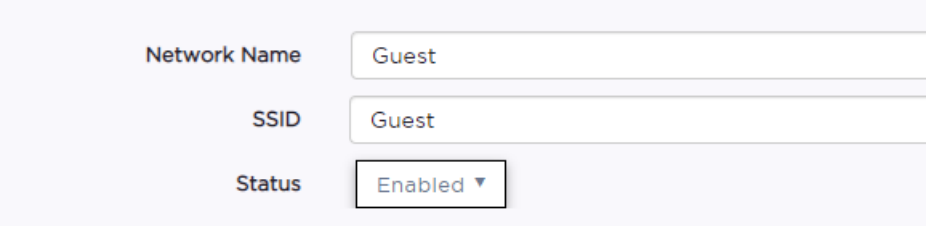


Figure 71: Network for Unregistered Policy

2. From ExtremeCloud IQ - Site Engine, go to **Access Control** > **Configuration** > **Profiles** > **Policy Mappings**.

3. Select **Switch to Advanced**.
4. Select the Unregistered Policy, then **Edit**.

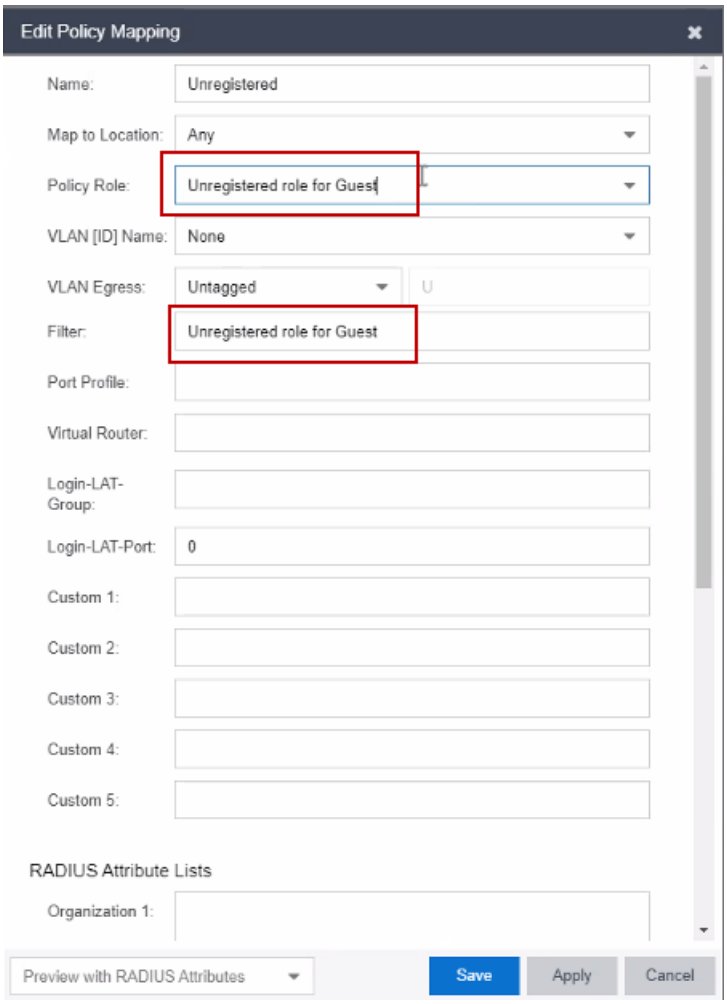


Figure 72: Referencing Unregistered Role from ExtremeCloud IQ Controller

Note
It is a best practice to specify *Unregistered role for <NETWORK NAME>* in both the **Policy Role** field and the **Filter** field. Depending on your configuration, either field can be referenced.

5. Enforce the changes.

   From **Engine Groups**, right-click the IP address of ExtremeCloud IQ Controller. Then, select **Enforce**.

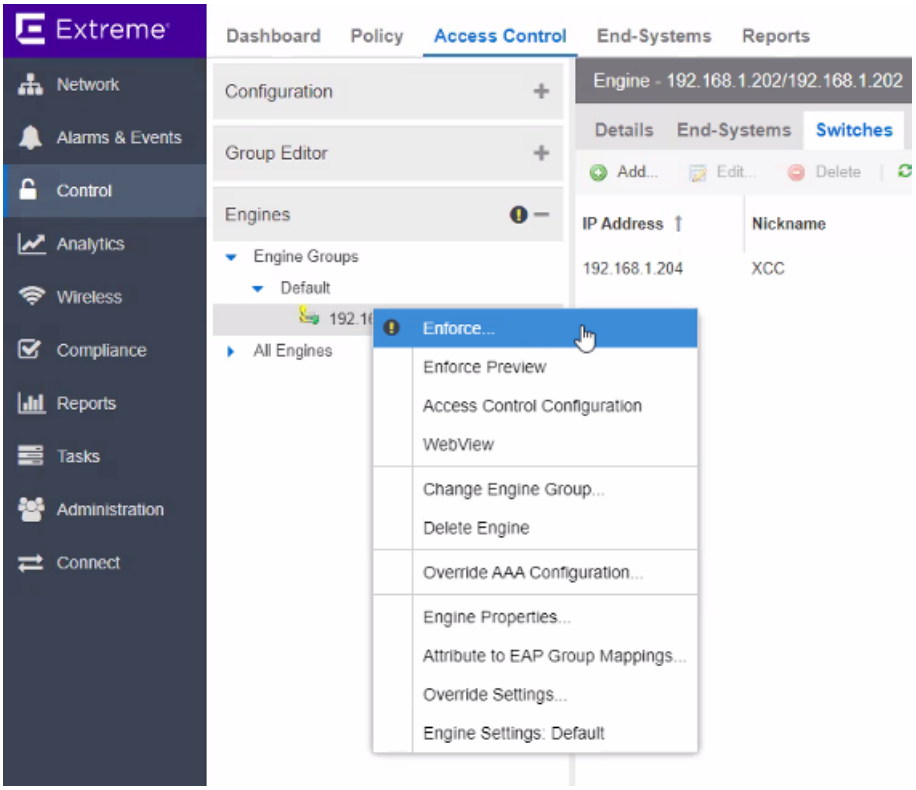


Figure 73: Enforce Changes

Editing the ExtremeCloud IQ - Site Engine Profile for Policy and Location-Based Services

In this section, we outline how to configure Location-Based Services in ExtremeCloud IQ - Site Engine to create more than one mapping to an External Captive Portal. Multiple mappings are necessary when configuring ExtremeCloud IQ Controller side-by-side with other controllers in your network.

All policies/filter-ids sent from ExtremeCloud IQ - Site Engine to ExtremeCloud IQ Controller must also be configured in ExtremeCloud IQ Controller. If ExtremeCloud IQ Controller cannot correlate a filter-id to an existing policy in the ExtremeCloud IQ Controller roles database, the ExtremeCloud IQ Controller default authenticated roles are applied.

To enable Location Based Services ExtremeCloud IQ - Site Engine, take the following steps:

1. Go to **Control** > **Access Control** > **Configuration**.
2. Select the configuration in use, then select **Rules**.
3. Select **Advanced Locations** > **Add**.
4. Select **Location Field** > **New**.

5. Select **Add**.

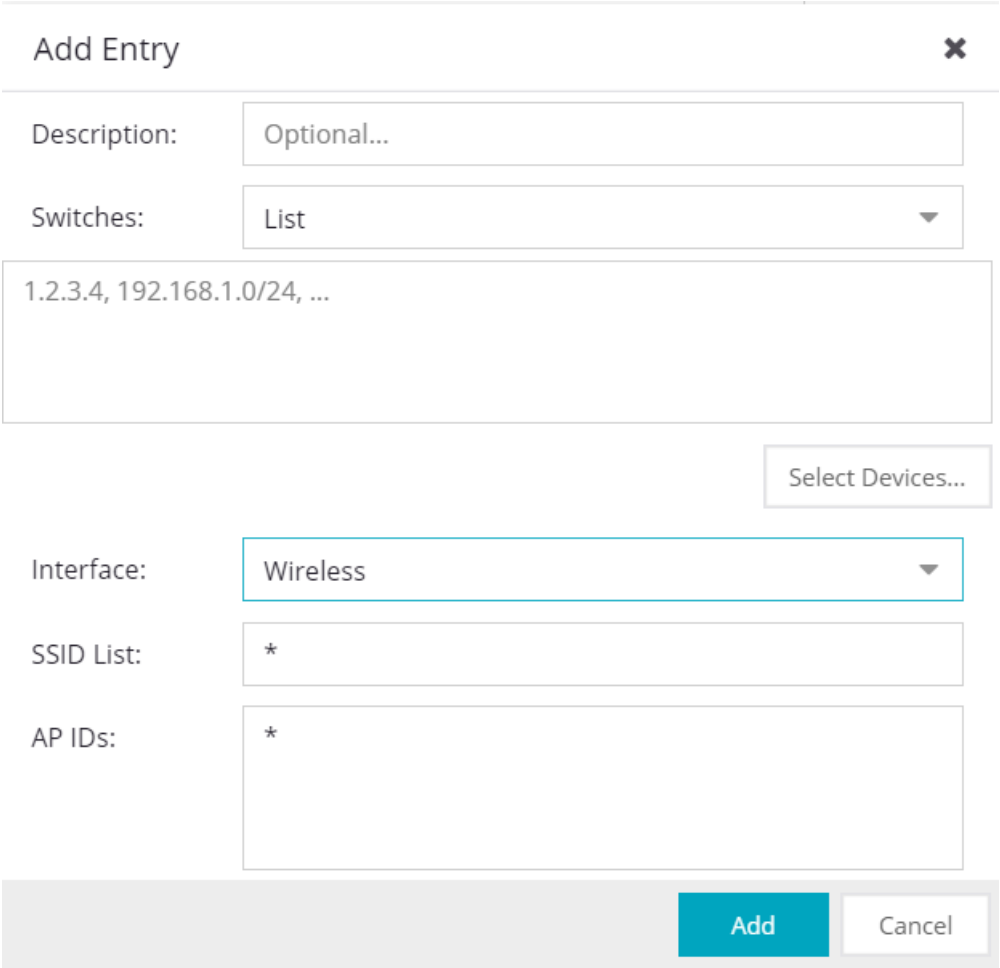


Figure 74: Add Location Group

6. Create the location group as follows:

   Switch

   ExtremeCloud IQ Controller Switch IP address. Use the **Select Devices** button to select one or more devices.

   Interface (optional)

   Select **Wireless** to restrict to a Wireless interface.

7. Select **Add**.

8. Select **Save** to save the group.

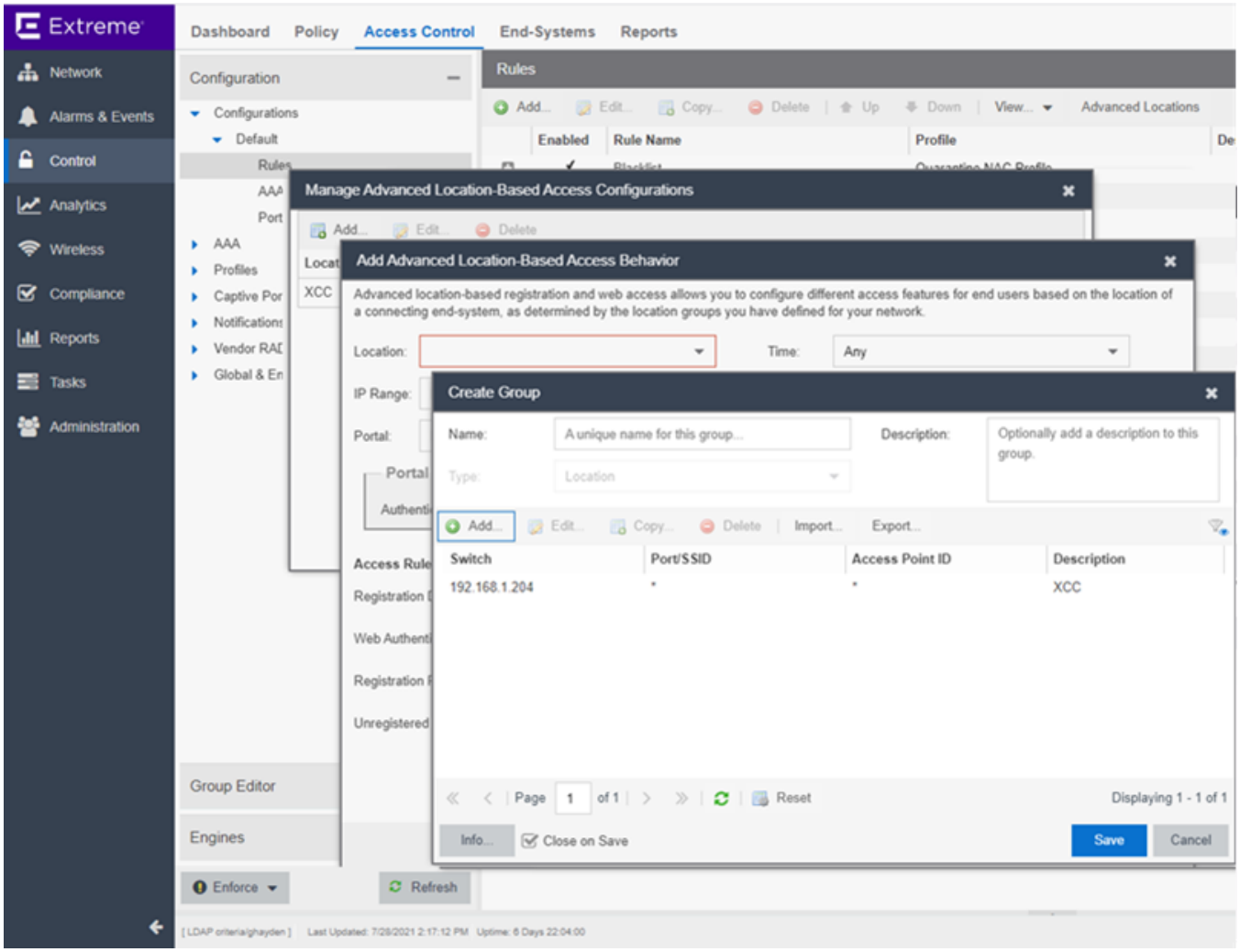


Figure 75: Create Location Group for ExtremeCloud IQ Controller

9. From the **Add Advanced Location Based Access Behavior** screen, select the newly created location group for the **Location** field, and select **OK**.

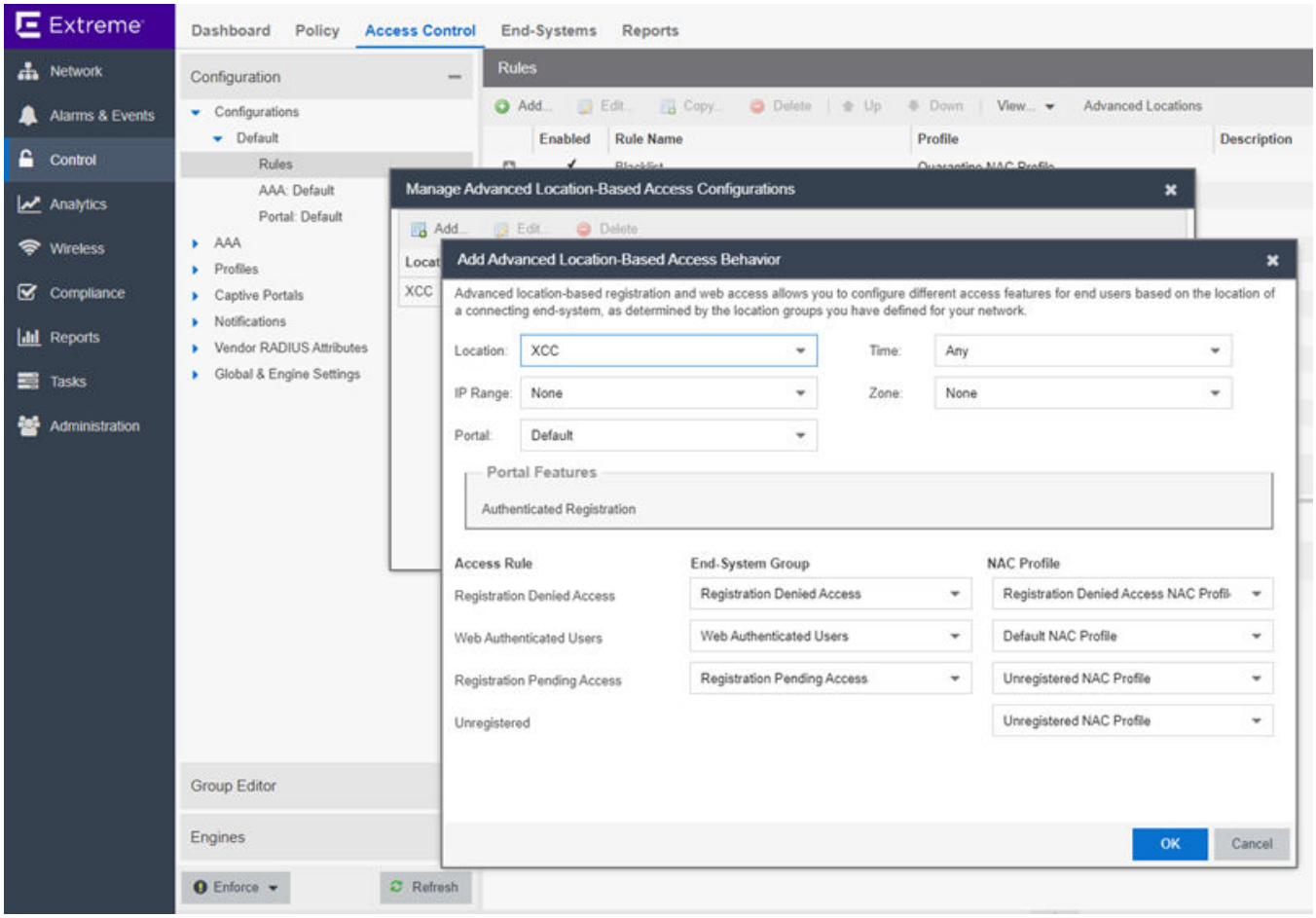


Figure 76: New Location Group for ExtremeCloud IQ Controller

10. Select the portal and features that you wish to enabled for this location.

> **Note**
> When a portal configuration is used in multiple advanced location based sets, edits to a portal in one set will propagate across all sets. For example, if you remove Guest Registration from the Default portal, Guest Registration is removed from all advanced location based portals that use are based on the Default portal.

11. From the Rules Engine, select the newly created Unregistered rule.
12. Now create a profile associated with the Unregistered ExtremeCloud IQ Controller rule.
    a. Double-click the new Unregistered Rule to open the **Edit Rule** dialog.
    b. Scroll down to the **Actions** pane and select the **Profile** field.
    c. From the Profile field, select **New**.

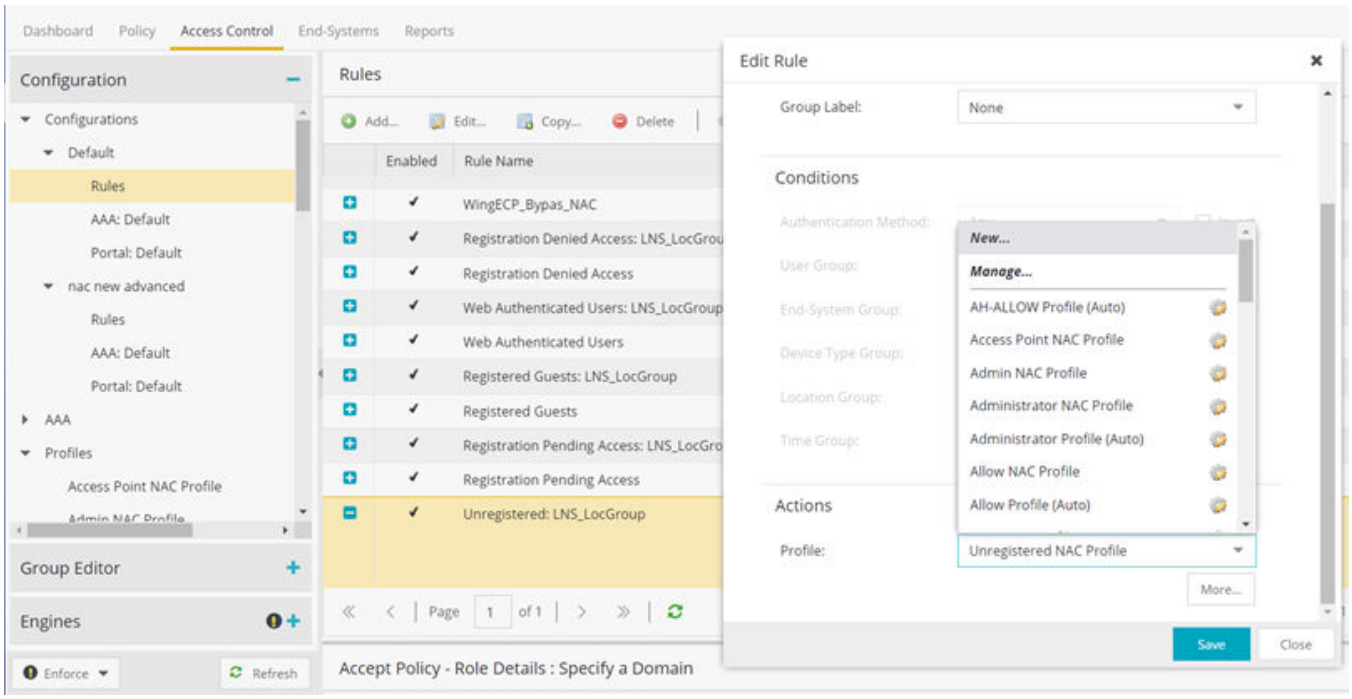


Figure 77: ExtremeCloud IQ Controller Policy Rule Mapping

13. Create a new profile called *Unregistered role for <Network Name>*. In our example we used **Guest**.
14. From the new profile, select **Accept Policy** > **New**.
15. Create a new policy mapping.

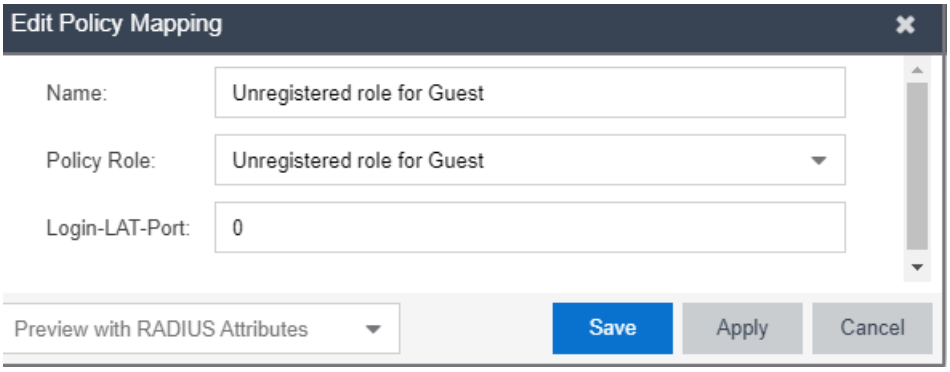


Figure 78: Edit Policy Mapping

16. Select newly created policy mapping as the Accept Policy.

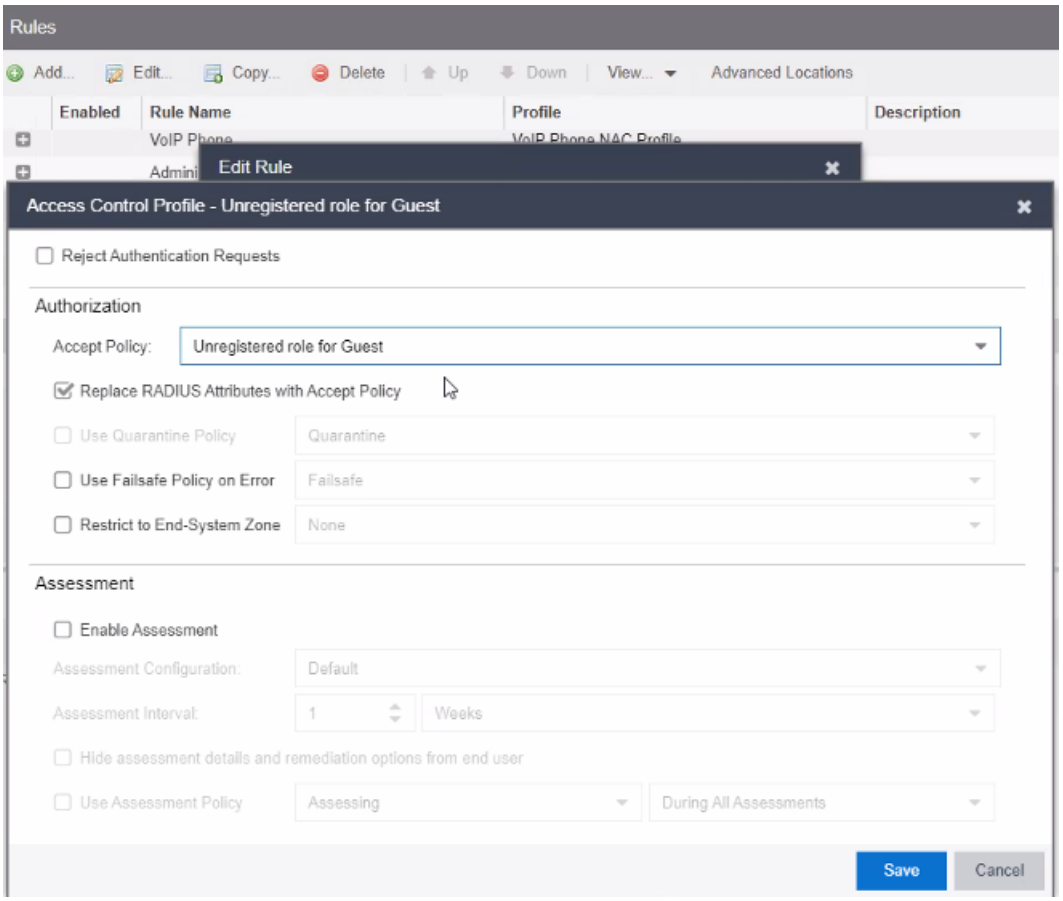


Figure 79: Profile Unregistered for Guest ExtremeCloud IQ Controller

Note
There are multiple registration rules for each registration type (rules ending with XCC and rules without the XCC suffix), because we have configured both Guest and Authenticated registrations enabled on the portal configuration.

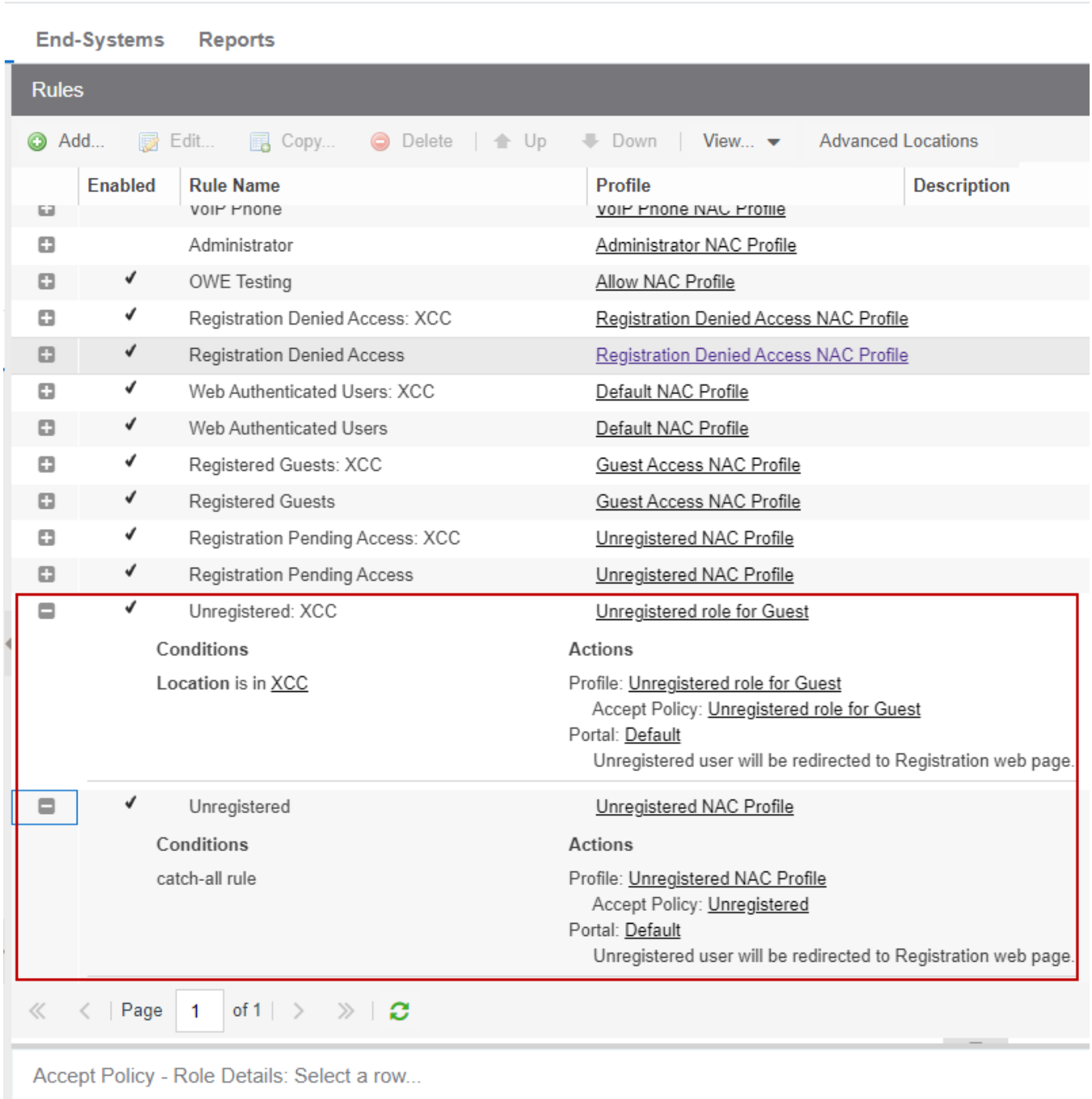


Figure 80: Final Rule Configuration

Note

If there is a mismatch in roles between Extreme Control and ExtremeCloud IQ Controller, force a re-authentication from ExtremeCloud IQ Controller. The mismatch may be a result of a timing issue. View **Session timeouts** on the network configuration for more information.

If the mismatch persists, confirm that you have used exact syntax on the role configuration. See Editing the Unregistered Policy on ExtremeCloud IQ - Site Engine on page 175 for more information.

For more information about External Captive Portal on ExtremeCloud IQ - Site Engine, refer to ExtremeCloud IQ - Site Engine Documentation.

Deploying an ExtremeGuest External Captive Portal

Configure an ExtremeGuest Server on page 186
Configure an ExtremeGuest Captive Portal Network on page 186
Configuration Settings on ExtremeGuest on page 187

Deployment Strategy

The following strategy outlines how to configure ExtremeCloud IQ Controller to integrate with ExtremeGuest™, which houses the external captive portal. The ExtremeGuest server can be assigned from the ExtremeCloud IQ Controller **Networks Add** page to handle client authentication and accounting. The portal resides on the ExtremeGuest server and ExtremeCloud IQ Controller initiates the client network connections.

The following outlines how to integrate ExtremeCloud IQ Controller with ExtremeGuest.

1. Add a site with a device group.
2. Configure one or more ExtremeGuest servers.
3. Configure a captive portal network:
   - Select **Enable Captive Portal** on the network.
   - Select portal type **EGuest**.
   - Specify the ExtremeGuest servers.
4. Modify the configuration profile associated with the device group:
   - Assign the ExtremeGuest network to the device group.
   - Assign the policy roles to the device group.

Note
The policy role names must match on both ExtremeGuest and ExtremeCloud IQ Controller. A simple approach is to create policies on ExtremeGuest with names that match the ExtremeCloud IQ Controller default policies.

Related Topics

Configure an ExtremeGuest Server on page 186
Configure an ExtremeGuest Captive Portal Network on page 186

Configuration Settings on ExtremeGuest on page 187

Configure an ExtremeGuest Server

Configure up to three ExtremeGuest servers. To configure an ExtremeGuest server. Take the following steps:

1. Go to **Configure** > **ExtremeGuest** and select **Add**.
2. Configure the following parameters:

   IP Address

   Valid IP address of the ExtremeGuest server.

   Name

   Name of the ExtremeGuest server.

   FQDN

   Fully-qualified domain name of the ExtremeGuest server.

   Authentication Timeout Duration (Seconds)

   Determines a timeout value, in seconds, for the RADIUS server connection.

   Authentication Retry Count

   Determines the number of times ExtremeCloud IQ Controller will attempt to authenticate an end user.

   Authentication Client UDP Port

   User Datagram Protocol (UDP) port number used for client authentication. UDP needs only one port for full-duplex, bidirectional traffic.

   Shared Secret

   The password that is used to validate the connection between ExtremeCloud IQ Controller and the ExtremeGuest server.

   Mask

   Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

   Callback User Name

   User ID that Callback Manager uses to access the ExtremeGuest server.

   Callback Password

   The password that Callback Manager uses to access the ExtremeGuest server. The minimum password length is 6 characters.

   Mask

   Determines if the Shared Secret or password value is displayed on the user interface. Enable Mask to display dots in place of the Shared Secret or password value. To display the password characters, clear the **Mask** check box.

Configure an ExtremeGuest Captive Portal Network

To configure an ExtremeGuest captive portal network.

Go to **Networks** > **Add** and configure the following parameters:

Network Name

ECA_EGuest

SSID

ECA_EGuest

Auth Type

Select **WPAv2 with PSK** then click **Edit Privacy** and enter a password key.

Enable Captive Portal

Check this option and specify the following parameters:

- Captive Portal Type = **EGuest**
- Select the ExtremeGuest server from the drop-down list of configured servers. The number of server fields depends on the number of configured servers. Configure one portal server and up to two backup servers.
  - Select an icon (, , or) to manage your servers from here. Select the appropriate check box to indicate that the server handles authentication, accounting, or both. At least one selection is required for each server.
  - Select **Portal** to configure one server as the portal server. If your portal server goes down, you must manually select a backup server as the portal server.

Note
Walled Garden rules are not required for this network. The process of enabling a captive portal on the network automatically creates rules allowing DNS, DHCP, and redirection rules. However, if users are unable to connect to the network, consider creating specific DNS and DHCP Allow rules as a Walled Garden configuration.

MAC-based authentication (MBA)

This option is enabled by default. Configure the following parameters:

MBA Timeout Role

Unregistered

Use HTTPS connection

Enable this option if connecting to the server through https.

Default Auth Role

Enterprise User

Default VLAN

Bridged at AP Untagged

Configuration Settings on ExtremeGuest

Configure the following settings on ExtremeGuest to support integration with ExtremeCloud IQ Controller:

- Policy Role Names — The policy role names must match on both ExtremeGuest and ExtremeCloud IQ Controller. A simple approach is to create policies on

ExtremeGuest with names that match the ExtremeCloud IQ Controller default policies.

- Configure ExtremeCloud IQ Controller as the **AAA NAS** (Network Access Server). Use the IP address (or Subnet address) of ExtremeCloud IQ Controller or the address of the RF Domain Manager.

For more information, see the *ExtremeGuest User Guide* on https://extremenetworks.com/support/documentation.

Deploying Client Bridge

AP Client Bridge on page 189
Configure Client Bridge on page 191

Deployment Strategy

The following strategy outlines how to configure an AP radio as a client bridge to ExtremeCloud IQ Controller. The bridge AP roams, functioning as a client of the root (infrastructure) AP. Client bridge enables end-system clients to roam while continuing to be connected to the infrastructure through the wireless network.

Related Topics

AP Client Bridge on page 189
Configure Client Bridge on page 191

AP Client Bridge

AP Client Bridge topology extends a wired LAN using a wireless network. The Client Bridge can be used to tunnel network traffic to ExtremeCloud IQ Controller, enabling connectivity for wired devices that are moved around a facility. For example, a medical device that is moved between rooms can maintain connectivity to ExtremeCloud IQ Controller through an AP radio configured as the uplink. The medical device moves with the Client Bridge AP, the two devices can be connected through the wired port (ETH1/GE2) or through a wireless connection. Client Bridge can be deployed for untagged traffic from an access port to a single VLAN on ExtremeCloud IQ Controller. (The wired port is associated with a single network.) Or, as a Transparent Bridge that supports a trunk port with tagged traffic to multiple VLANs.

For more information, see Configure Transparent Bridge on page 80.

The Client Bridge deployment includes one or more infrastructure APs. After provisioning, the Client AP connects to normal infrastructure services. The infrastructure AP is essentially any AP deployed for standard service offering. The infrastructure APs communicate with the ExtremeCloud IQ Controller supporting the usual traffic flow. The Client Bridge AP roams like a wireless client, supporting background scanning to determine available infrastructure APs. The Client Bridge AP associates on the infrastructure AP SSID (using network credentials) establishing a Client Bridge link with the infrastructure.

Client Bridge AP is adopted by ExtremeCloud IQ Controller and is managed as any other AP:

- When the Client Bridge AP is in *Client* mode (i.e. the GE2 port is set to **Client**), the wired clients connected to Client Bridge AP are controlled by the same policies as the wireless clients that are connected to any other AP.
- When the Client Bridge AP is in *Transparent Bridge* mode (i.e. the GE2 port is set to **Bridge**), the Client Bridge AP is transparently forwarding all traffic without monitoring individual sessions.

To get started, configure the Client Bridge settings on ExtremeCloud IQ Controller. Configure the Client Bridge from the configuration Profile. The Client Bridge AP is a member of a device group that references a Profile configured for Client Bridge.

Define Client Bridge from the **Radios** tab within the configuration Profile. Only one radio can be configured as a Client Bridge. This can be either radio. Regardless of which radio is configured as the Client Bridge, both radios will continue to provide service.

Client Bridge and Transparent Bridge are supported on Wi-Fi 6 AP models:

- Wi-Fi 6E World-Wide Universal APs ExtremeCloud IQ or on-premise operation
- Wi-Fi 6 Universal APs ExtremeCloud IQ or on-premise operation
- Wi-Fi 6 on-premise operation only.

.

Note
The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port.

Note
For ExtremeCloud IQ Controller deployments with network policy assignment for proper end-system visibility, the Client Bridge AP must be in a Centralized Site (Campus mode) and must be managed by ExtremeCloud IQ Controller.

Wired and wireless clients can be managed by Client Bridge. Client traffic can be forwarded on any of the following supported topologies: Bridged@AP, Bridged@AC, Fabric Attach, and VxLAN. A wired client refers to a device that has direct wired connectivity to the client port (GE2) of the AP. This can be a direct connection into

the AP port or connected through a layer 2 switch. The wired client port supports up to 128 simultaneous client sessions.

Note

- The following AP models with PSE provide downstream POE:
  - AP5010 — PSE controlled from the user interface, and it is available only when the AP is powered from BT.
  - AP302W and AP310i/e — PSE is switched on automatically when the AP is powered from AT.
- Ports on the Universal APs are labeled with the prefix ETH.
- When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.

Network policy is applied to both wired and wireless clients in the same way. The network policy is enforced on the Client Bridge AP before the network traffic is forwarded. All configuration updates are pushed to the Client Bridge AP before being applied to the infrastructure AP.

The role assignment for each AP is defined in its unique configuration Profile. When using Bridged@AP and Fabric Attach topologies, ensure that the Client Bridge role assignment is synchronized with the infrastructure AP role assignment.

Note

For a Client Bridge path, policy enforcement for clients is handled at the Client Bridged AP, including any adjustments to topology assignment (VLAN Tagging). The infrastructure AP operates purely as a transparent bridge for the traffic that is received from the Client Bridge AP. The same applies to management network access. If the infrastructure is configured to require management traffic on a specific VLAN, and is tagged by the infrastructure AP, the same configuration needs to be applied to each Client Bridge AP, ensuring that the VLAN tags match the infrastructure requirement. It behaves essentially as if the Client Bridge access point was directly connected to the same infrastructure switch port as the infrastructure AP that provides the path for wireless connectivity.

Related Topics

Configure Client Bridge on page 191

Configure Client Bridge

Use a Client Bridge to extend a wired LAN using a wireless infrastructure. To configure a Client Bridge to work with ExtremeCloud IQ Controller take the following steps:

1. From ExtremeCloud IQ Controller, create a device group for your Client Bridge AP.
2. For RF Management, select **Default Smart RF**.

3. Edit the default configuration Profile for the AP model, specifying the client bridge settings.

   To edit the configuration Profile, select .

4. From the **Radios** tab, select **Client Bridge** as the Radio Mode value for either radio.

   Note

   Consider the following when configuring a radio as a Client Bridge:

   - Only one radio can be configured as a Client Bridge. This can be either radio. Regardless of which radio is configured as the Client Bridge, both radios will continue to provide service.
     - Radio 1 enables Client Bridge on the 2.4GHz band only.
     - Radio 2 enables Client Bridge on the 5GHz band only.
   - The Client Bridge radio will connect on the radio channel that is determined by the infrastructure AP.
   - When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.
   - Eight networks can be configured per radio. If one network is configured as a Client Bridge, seven additional networks can be configured for service on that radio.

5. Select the **Client Bridge Network**.

   The following WLAN parameters are passed to the Client Bridge AP to configure station mode on the radio:

   - Network SSID
   - Encryption or Authentication type
   - Pre-shared key

   The selected network must be configured with one of the following supported authentication types:

   - Open
   - WPA2-Personal (PSK)
   - WPA2-Enterprise 802.1x/EAP
   - WPA3-Enterprise 802.1x/EAP
   - MAC-base Authentication (MBA)

   When using authentication types **WPA2-Enterprise 802.1x/EAP** and **WPA3-Enterprise 802.1x/EAP**, select the icon to configure the user ID and password.

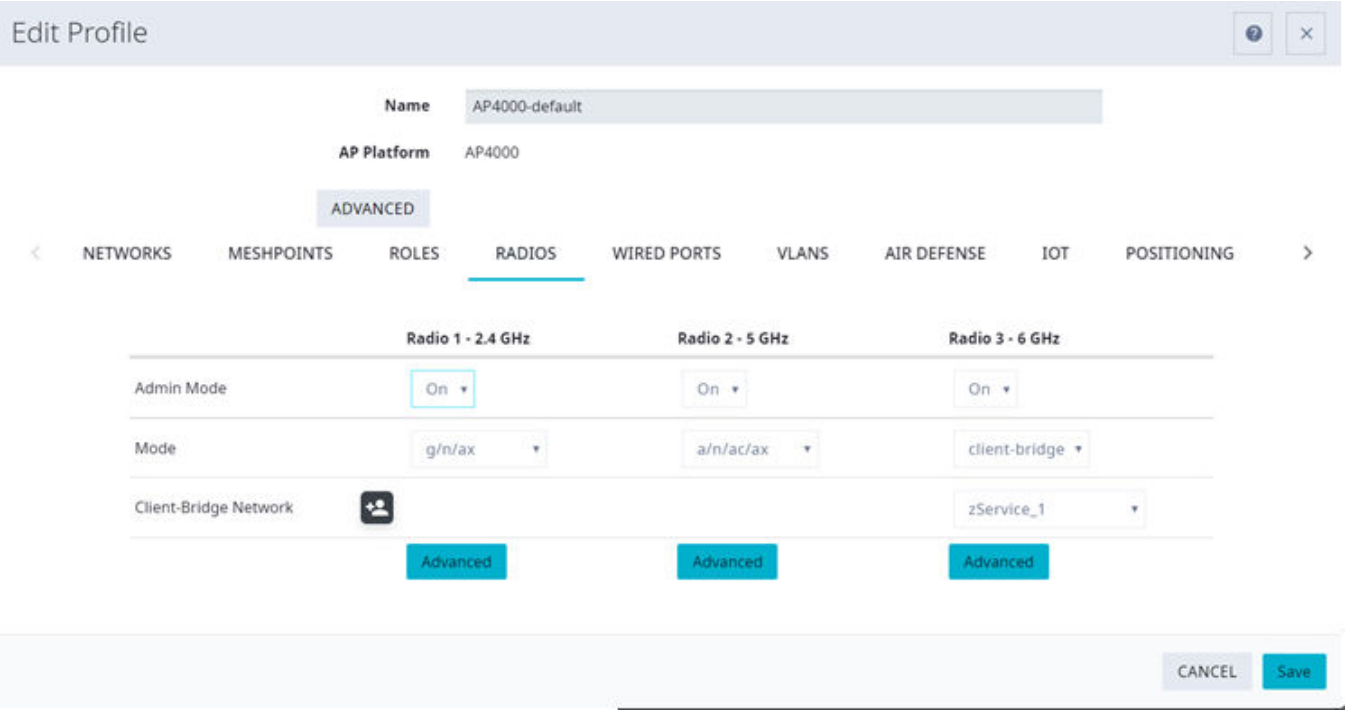


Figure 81: Configuration Profile with Client Bridge Configuration

Note
A Client Bridge AP will *not* associate to the infrastructure network with authentication types Open or WPA2-Personal (PSK) in combination with captive portal. These scenarios require user interaction.

Note
The Client Bridge network and the infrastructure AP network must match on the same radio. On the Client Bridge AP, if the 2.4 GHz radio is configured as Client Bridge, the infrastructure AP must broadcast that network on a 2.4GHz radio.

6. From the configuration Profile **Advanced** settings, the **GE2 Port Function** is automatically set to **Client** after configuring the Client Bridge radio.

   To configure a transparent point-to-point bridge that supports tagged traffic, set the **GE2 Port Function** to **Bridge**.

   Note
   - The ETH1/GE2 Bridge port is *not* supported on access points with a single Ethernet port.
   - Ports on the Universal APs are labeled with the prefix ETH.
   - When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.

7. Save the configuration Profile.
8. If you are planning to connect the end-system to the Client Bridge AP through the GE2 port, edit the configuration Profile again.
9. On the **Networks** tab, the Client Bridge network is indicated with a black highlight.

   Note
   The Client Bridge is always assigned the primary BSSID (Basic Service Set Identifier). If you change the Client Bridge network assignment, the radio is reset, resulting in a service interruption.

10. On the **Networks** tab, select **GE2** port.

    Only allow one network assignment to Client Bridge and GE2 interfaces respectively.

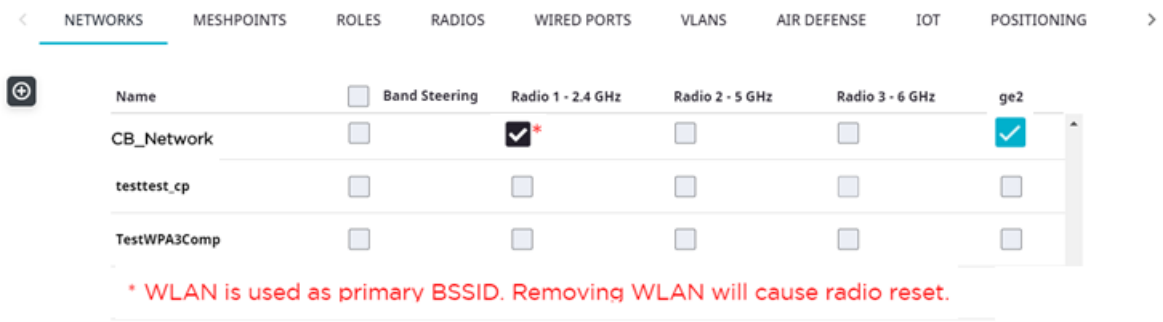


Figure 82: Configuration Profile Network Configuration – Client Bridge

11. Connect the Client Bridge AP to ExtremeCloud IQ Controller using the GE1 Port, which is designated as the primary port.
12. Assign the Client Bridge AP to the device group and assign the device group to the site.
13. After the Client Bridge link is established, disconnect the Client Bridge AP from the GE1 Port and ExtremeCloud IQ Controller.

    After the bridge is established, you can find the Client Bridge AP on the **Clients List**.

The end-system device traffic is connected through GE2 port (or ETH/POE port for the single interface). The Client Bridge AP communicates with the infrastructure AP on the wireless network.

When Client Bridge is configured on a single interface AP, the single interface is used as the client port, not as an uplink, and you will not see the **GE2 Port Function** field in the configuration Profile **Advanced Settings**.

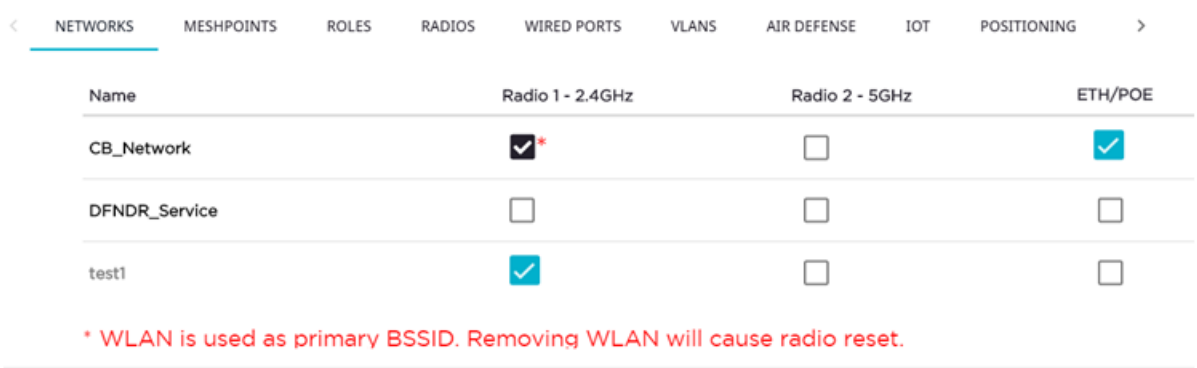


Figure 83: Configuration Profile Network Configuration – Client Bridge on a single interface AP

The wired port speed is configured on the **Wired Ports** tab.

Related Topics

Configure Transparent Bridge on page 80
AP Client Bridge on page 189

Deploying an Availability Pair

ExtremeCloud IQ Controller provides the availability feature to maintain service availability in the event of an outage. The Availability Pair feature allows both AP and Client statistics to be available on both sides of the High Availability configuration.

Before you begin:

1. Enable NTP on both ExtremeCloud IQ Controller appliances. Go to **Administration** > **System** > **Network Time** and select **NTP**.
2. On the primary ExtremeCloud IQ Controller, go to **Administration** > **System** > **Availability** and select **Paired**.
3. Configure the following parameters:

   Role

   Primary

   Peer IP Address

   The data port IP address of the second ExtremeCloud IQ Controller.

   Note
   The Peer IP address must refer to a physical topology of the peer appliance. It can be the IP address of a physical port or the IP address of a Lagged interface. Configuring availability against a service topology such as the IP address (L3) of a Bridged@Controller appliance is not supported.

   Auto AP Balancing

   Select **Active - Passive**

   In a Availability Pair, an AP establishes an active tunnel to one appliance and a backup tunnel to the other appliance. The active tunnel is used to pass the client data over tunneled topologies.

   - In an **Active-Active** configuration, approximately half of the APs establish an active tunnel to the primary appliance. The remaining APs establish an active tunnel to the backup appliance, spreading the load across the Availability Pair.
   - In an **Active-Passive** configuration, all APs establish an active tunnel to the primary appliance. The secondary appliance is used for failover only.

     In either configuration, however, most parameters can be configured on either appliance in the availability pair.
4. Click **Save**.

5. On the secondary ExtremeCloud IQ Controller, select **Paired** and configure the following parameters:

   Role

   Backup

   Pair IP Address

   The IP address of the primary ExtremeCloud IQ Controller.

   Auto AP Balancing

   Select **Active-Passive**
6. Click **Save**.
7. Go to **Admin** > **Logs** and look for the message `Availability Link established with Peer <ip address>`.

   Note
   It will take a few minutes for the two ExtremeCloud IQ Controller configurations to synchronize.

8. To verify synchronization, view the Network Health widget from the Diagnostics dashboard. Go to **Tools** > **Diagnostics** > **Dashboard**.

   Or, add a network health widget to the Overview dashboard:

   a. Go to **Dashboard**.
   b. Select to edit the dashboard.
   c. Select **Widgets**.
   d. Select **System** and drag **Network Health** onto the dashboard.

   The **Synchronization Status** is displayed as part of the Network Health widget.

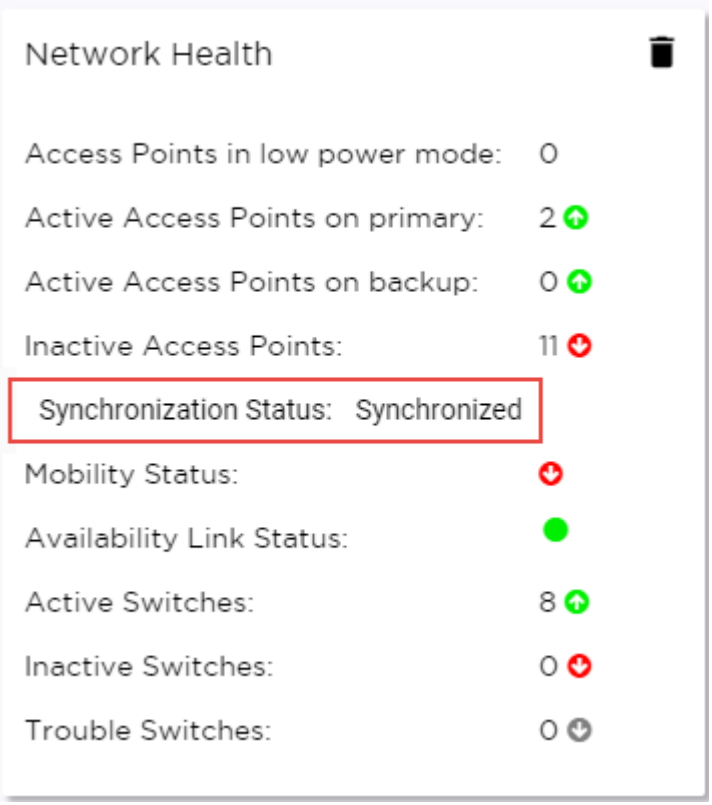


Figure 84: Availability Pair Synchronization Status

Note
In a High Availability Pair, onboard the primary controller only to ExtremeCloud IQ for Cloud Visibility. For more information, see Onboard a Controller to ExtremeCloud IQ on page 213.

Deploying an Availability Pair with Extreme AirDefense

Deployment Procedure on page 199
Configuring the Centralized Site with an AP3915 Profile on page 200
Configuring AirDefense on page 200

Deployment Strategy

The following scenario outlines an availability pair of ExtremeCloud IQ Controller appliances that utilize ExtremeWireless access point models. This scenario supports integration with Extreme AirDefense.

This deployment scenario offers the following configuration factors:

- Availability pair of ExtremeCloud IQ Controller appliances.
- Appliance capacity 32K-100K users
- Local authentication with 802.1x and internal captive portal.
- AirDefense is provisioned from within ExtremeCloud IQ Controller and the data is fed from the APs.

Deployment Procedure

1. Create a site with a device group for the AP3915 devices.
2. Configure an internal captive portal.
3. Specify the network topology.
4. Configure a captive portal network.
5. Work with the captive portal engine rules.
6. Go back to each device group in the site and configure the configuration profile.
7. Create adoption rules for each device group.
8. Deploy the availability pair.

Related Topics

Adding a Centralized Site with Device Group on page 57
Configuring an Internal Captive Portal on page 59
Specifying B@AC Network Topology on page 60
Configuring a Captive Portal Network on page 61

Working with Internal Captive Portal Engine Rules on page 62
Configuring the Centralized Site with an AP3915 Profile on page 200
Creating Adoption Rules on page 65
Deploying an Availability Pair on page 196

Configuring the Centralized Site with an AP3915 Profile

1. Go to **Configure** > **Sites** > **Add** to create a Centralized site.
2. Click **Device Groups**.
3. Select the AP3915 device group.
4. From the Profile field, select the **default AP3915** profile and click to edit the profile.
5. From the **Networks** tab, select the configured Internal Captive Portal network.
6. From the **Roles** tab, select the configured policy roles.
7. From the **AirDefense** tab, configure AirDefense integration.

Related Topics

Adding a Centralized Site with Device Group on page 57
Editing Device Group Profile for Network and Role on page 63
Configuring AirDefense on page 200

Configuring AirDefense

The AP integrates with the AirDefense Service Platform (ADSP), offering an additional profile option that allows the AP to function as an AirDefense sensor or to act as a sensor and retain the ability to forward traffic.

In dedicated sensor mode, the AP operates independently from the ExtremeCloud IQ Controller while the ExtremeCloud IQ Controller continues to see the AP and display the AP Role as a dedicated AirDefense sensor. In its role as a dedicated sensor, the AP does not report statistics to the ExtremeCloud IQ Controller.

Table 22: AirDefense Profile Settings

Field	Description
Name	Name of AirDefense profile.
Add Server Address	The IP address of the AirDefense servers. Provide the FQDN or IPv4 string, maximum 255 characters. Enter the IP address, then click . The IP address is added to the **Servers** list. **Note:** When using the AirDefense Base (add-on container application), provide the IP address of the ExtremeCloud IQ Controller data port that is reachable by the APs and sensors.

Table 22: AirDefense Profile Settings (continued)

Field	Description
Port	Specify a port for the AirDefense server. The default port is 443 (used with a dedicated external AirDefense Server). **Note:** When using the AirDefense Base (add-on container application), configure port number to **32032**.
Servers	List of IP addresses for servers. Click 🗑 to remove an IP address from the list.

Deploying an Availability Pair and External Captive Portal

Deployment Procedure on page 202
Configuring External Captive Portal Network on page 203
Editing the Device Group Profile for ECP Network on page 206

Deployment Strategy

The following scenario outlines an availability pair of ExtremeCloud IQ Controller appliances with ExtremeWireless access point models. This scenario employs an External Captive Portal.

This deployment scenario offers the following configuration factors:

- Availability pair of ExtremeCloud IQ Controller appliances
- Appliance capacity 32K-100K users
- MBA with local authentication and External Captive Portal.

Related Topics

Deployment Procedure on page 202
Configuring External Captive Portal Network on page 203

Deployment Procedure

1. Create a site with a device group for the AP3915 devices.
2. Configure an External Captive Portal.
3. Specify the network topology.

   Specify **Bridged@AP**. ExtremeWireless APs support both Bridged@AC and Bridged@AP topologies.
4. Configure an External Captive Portal network.
5. Engine Rules: The ExtremeCloud IQ Controller rules engine generates a default Unauthenticated rule. There is no user interaction required on the ExtremeCloud IQ Controller. An authenticated rule is generated from the External Captive Portal server. You must define a policy role on ExtremeCloud IQ Controller that matches the authenticated role on the server. This can be a unique role or default authenticated role like Enterprise User.

6. Go back to each device group and configure the configuration profile. Specify the External Captive Portal network and the ExtremeCloud IQ Controller authenticated role that matches the ECP server authenticated policy.
7. Create adoption rules for each device group.
8. Deploy the availability pair.

Related Topics

Adding a Centralized Site with Device Group on page 57
Configuring External Captive Portal Network on page 203
Creating Adoption Rules on page 65
Deploying an Availability Pair on page 196

Configuring External Captive Portal Network

To configure an External Captive Portal network:

1. Go to **Configure** > **Networks** > **WLANS** > **Add**
2. Configure the following parameters:

Table 23: External Captive Portal Settings

Field	Description
Network Name	Enter a unique, user-friendly value that makes sense for your business. Example: Staff
SSID	Enter a character string to identify the wireless network. Maximum 32 characters. Upper and lowercase allowed. Example: PermanentStaff
Status	Enable or disable the network service. Disabling the network service shuts off the service but does not delete it.

Table 23: External Captive Portal Settings (continued)

Field	Description
Auth Type	Define the authorization type. Valid values are: • Open —Anyone is authorized to use the network. This authorization type has no encryption. The Default Auth role is the only supported policy role. • WEP — Static Wired Equivalent Privacy (WEP) offers keys for a selected network, that match the WEP mechanism used on the rest of the network. Each AP can participate in up to 50 networks. Specify one WEP key per network. This option is offered to support legacy APs. • WPA2 with PSK — Network access is allowed to any client that knows the pre-shared key (PSK). All data between the client and the AP is AES encrypted using the shared secret. Privacy is based on the IEEE standard, and privacy settings are editable. If MAC-based authentication (MBA) is enabled, you can assign different roles to different devices with a PSK because MBA distinguishes between different devices. If MBA is not enabled, then devices with a PSK use the Default Auth role only. • WPA2 Enterprise w/ RADIUS — Supports 802.1X authentication with a RADIUS server, using AES encryption. This method can be used with client certificate-based authentication (EAP-TLS). All 802.1X protocols are supported. **Note:** Captive Portal is not supported when using WPA2 Enterprise w/ RADIUS. An exception is *Centralized Web Authentication (CWA)*. CWA captive portal supports WPA2 Enterprise w/ RADIUS. **Privacy Settings** Protected Management Frames — Management Frames are the signaling packets used in the 802.11 wireless standard to allow a device to negotiate with an AP. PMF adds an integrity check to control packets being sent between the client and the access point. Valid values are: ◦ Enabled. Supports PMF format but does not require it. ◦ Disabled. Does not address PMF format. Clients connect regardless of format. ◦ Required. Requires all devices use PMF format. This could result in older devices not connecting. • WPA3 - Personal — 128-bit encryption. ◦ AP3xx running ExtremeWireless WiNG 7.3x and later.

Table 23: External Captive Portal Settings (continued)

Field	Description
	◦ AP4xx running ExtremeWireless WiNG 7.3x and later. ◦ AP5xx running ExtremeWireless WiNG 7.2x and later. WPA3 uses a pre-shared key (PSK) and Simultaneous Authentication of Equals (SAE) or Hash-to-Element (H2E). WPA3 offers an augmented handshake and protection against future password compromises. • WPA3-Compatibility — Option for mixed deployments of 802.11ax APs and older AP models. For use when WPA2 and WPA3 are configured on the same network. Clients that support either WPA3 Personal or WPA2 Personal can connect to this network at the same time and on the same SSID. If you are unsure which method your device supports, use WPA3-Compatibility. Note: When a device is assigned to 6 GHz radio, only WPA3 Personal is assigned. For more information, see the *ExtremeCloud IQ Controller User Guide* or *Online Help*.
Enable Captive Portal	Check this option to enable captive portal support on the network service.
Captive Portal Type	Select **External** as the Captive Portal Type.
ECP URL	URL address for the external captive portal.
Walled Garden Rules	Select **Walled Garden Rules** to configure policy rules for the external captive portal.
Identity	Determines the name common to both the ExtremeCloud IQ Controller and the external Web server if you want to encrypt the information passed between the ExtremeCloud IQ Controller and the external Web server. Required for signing the redirected URL. If you do not configure the Identity, the redirector on the AP drops the traffic.
Shared Secret	The password that is used to validate the connection between the client and the RADIUS server.
Use HTTPS for connection	Indicates that the connection will be secure with HTTPS.
Send Successful Login To	Indicates destination of authenticated user. Valid values are: • Original Destination. The destination of the original request. • Custom URL. Provide the URL address.
MAC-based authentication (MBA)	Check this option to enable MBA.

3. Select **Save**.

Next, edit the configuration profiles in each device group, specifying the External Captive Portal network.

Related Topics

Editing the Device Group Profile for ECP Network on page 206

Editing the Device Group Profile for ECP Network

Configure an ECP network and be aware of the authenticated policy role that you are using before modifying the device group profile.

1. Go to **Configure** > **Sites** and select a site.
2. Click **Device Groups**.
3. Select a device group.
4. Beside the Profile field, select ✎ to edit the default profile AP3915-default.
5. From the **Networks** tab, assign a radio to the ECP network you created.
6. External Captive Portal networks use the Unregistered policy by default, there is no user interaction. The authenticated policy is configured on the captive portal server. You must specify an authenticated policy on the ExtremeCloud IQ Controller that will coincide with the authenticated captive portal server policy. For example, from the **Roles** tab, specify **Enterprise User** as the ExtremeCloud IQ Controller authenticated policy.
7. Optionally, you can configure settings from any of the available profile options. All APs in the device group are affected by options configured in the profile.

   Note
   The supported profile options depend on the AP Platform definition.

8. Click **Save** to save the profile settings.
9. Click **Close** to close the device group.

Next, configure adoption rules and deploy an availability pair of appliances.

Related Topics

Creating Adoption Rules on page 65
Deploying an Availability Pair on page 196

Integration with ExtremeCloud IQ

Deploy Universal APs on page 207
Onboard a Controller to ExtremeCloud IQ on page 213
Access the Controller UI from ExtremeCloud IQ on page 218

Extreme Networks offers universal APs that can be managed with an on-premise controller or managed with ExtremeCloud IQ. Additionally, you can onboard ExtremeCloud IQ Controller into ExtremeCloud IQ and take advantage of Cloud Visibility. After ExtremeCloud IQ Controller is onboarded into the cloud, all access points that are discovered by that controller are visible in ExtremeCloud IQ. This is not limited to Universal APs.

Next, select the controller to access the ExtremeCloud IQ Controller user interface and manage your devices, all from one pane of glass.

This chapter outlines how to deploy Universal Access Points, how to deploy the on-premise ExtremeCloud IQ Controller into ExtremeCloud IQ, and how to access the controller user interface from ExtremeCloud IQ.

Related Topics

Deploy Universal APs on page 207
Onboard a Controller to ExtremeCloud IQ on page 213
Access the Controller UI from ExtremeCloud IQ on page 218

Deploy Universal APs

The following Wi-Fi 6 access points can operate in either ExtremeCloud™ IQ or in an on-premise environment — one configured operating mode at a time.

- AP3000/X
- AP302W
- AP305C/CX
- AP305C-1
- AP4000
- AP4000-1
- AP410C
- AP410C-1

- AP460C/S6C/S12C
- AP5010
- AP5050U/AP5050D

ExtremeCloud IQ validates that the device is a Universal AP based on the serial number. The ExtremeCloud IQ onboarding logic checks both the model number and manufacturing date.

Universal Access Point Serial Number schema (14 Digits): XXXXYYMMDDnnnn

XXXX: Product Code

YYMMDD: Manufacturing Date Code

nnnn: Sequential Number (0001 – 9999)

- AP305C/CX

  Minimum serial number required for the AP305C and AP305CX access point model support:
  - First 305C SN = 03052009040001
  - First 305CX SN = 13052009040001
- AP410C

  Minimum serial number is required for AP410C access point model support:
  - First 410C SN = 04102101280001
- AP460C/S6C/S12C

  Minimum serial number is required for AP460C access point model support:
  - First 460C SN = 24602101250001
  - First 460S6C SN = 34602101250001
  - First 460S12C SN = 44602101250001

Related Topics

Onboarding Universal APs — ExtremeCloud IQ on page 208

Onboarding Universal APs — ExtremeCloud IQ

Universal APs are configured for cloud management by default. If you want to manage these APs locally, you must specify **Local Management** when onboarding the APs in ExtremeCloud IQ.

Note
To get a free ExtremeCloud IQ account, go to http://www.extremecloudiq.com.

To onboard your cloud-ready APs for Local Management with ExtremeCloud IQ Controller, take the following steps:

1. Log into your ExtremeCloud IQ account and select
   The **Welcome** dialog displays.

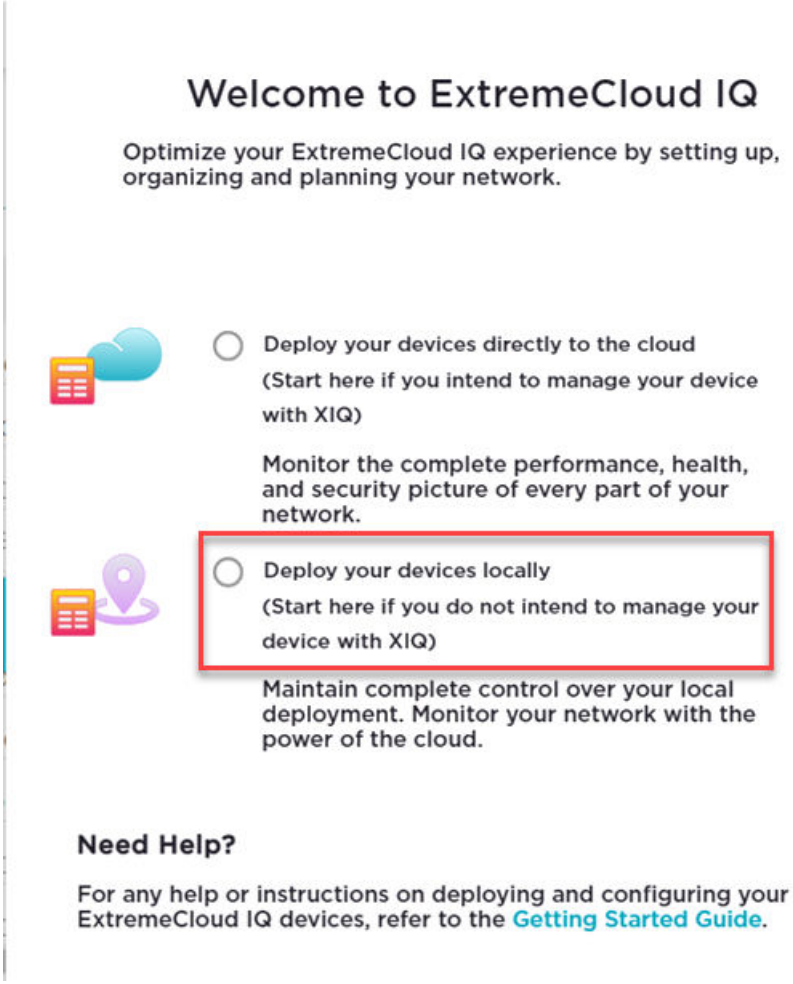


Figure 85: ExtremeCloud IQ Welcome Dialog

2. For on-premise management, select **Deploy your devices locally**.
3. On the next screen, select **Let's Get Started**.
4. Enter the Universal AP serial numbers:
   Serial numbers are available on the back of the AP or on the AP box label. In most cases, the invoice provided by the distributor includes the serial number of the devices fulfilled with the order. The ExtremeCloud IQ onboarding logic validates the serial numbers against the model compatibility and manufacturing date to ensure only compatible devices are onboarded.

   See Deploy Universal APs on page 207 for a list of minimum serial numbers that are supported by ExtremeCloud IQ Controller for specific Universal AP models.

   - Type in serial numbers of the Universal APs, separated by commas. See Local Onboarding — Manual Entry on page 212. Or,

- Import from a CSV file. See Local Onboarding— Import CSV file on page 213.

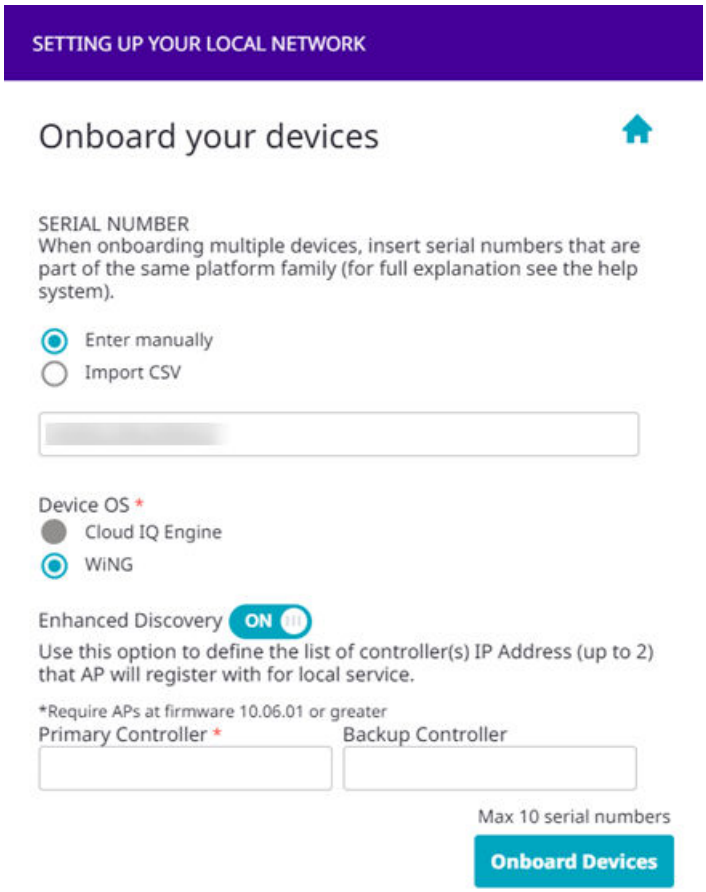


Figure 86: Onboarding your devices

5. **Enhanced Discovery**. Enhanced Discovery can be used to onboard a Universal Access Point to ExtremeCloud IQ for local management. For more information, see Enhanced Discovery on page 211.

   Note
   Enhanced Discovery is supported on AP3000. It requires ExtremeCloud IQ version 23.6.1 or greater.

6. Select **Onboard Devices**.
7. Select **Finish**.

   The APs display on the ExtremeCloud IQ Device List with the status **Onboarded**. New APs display the generic *HOSTNAME* because they are not yet registered with ExtremeCloud IQ. The AP Hostname automatically updates after the AP is powered on and connected into ExtremeCloud IQ.
8. Connect the AP to the network.

   Connect the AP to a switch through (ETH0/POE+). The AP hostname is recognized after the AP connects. It starts in the WiNG 7 operating system and discovers the ExtremeCloud IQ Controller provided that you have configured the necessary DHCP and DNS options.

The following are ExtremeCloud IQ Controller discovery options:

DHCP

- Option 78: Points to SLP DA, which is typically instantiated within the appliance itself.
- Option 43/60: Can point directly to the appliance, but would require double encoding of code points for Centralized (01). DHCP Server may not allow overload.

DNS

Controller. Resolves to the appliance IP address.

- DNS A-record : **controller**.<yourdomain>
- #option slp-discovery-agent true <eca_ip_address>

Multicast

SLP Multicast

For more information about configuring standard ExtremeCloud IQ Controller discovery options, see Configuring DHCP, NPS, and DNS Services on page 25.

After the AP discovers ExtremeCloud IQ Controller, it is displayed as **Unassigned** on the ExtremeCloud IQ Controller **Devices List**.

9. Refer to the *ExtremeCloud IQ Controller User Guide* for information about the following procedures:
   a. Creating a device group for each Universal AP model associated with a site.
   b. Associating a configuration Profile to each device group. The configuration Profile includes defined networks and operational settings required for service.
   c. Assigning each AP to the appropriate device group.

Related Topics

Enhanced Discovery on page 211
Deploy Universal APs on page 207
Configuring DHCP, NPS, and DNS Services on page 25
Onboard a Controller to ExtremeCloud IQ on page 213

Enhanced Discovery

Enhanced Discovery can be used to onboard a Universal Access Point to ExtremeCloud IQ for local management.

To support deployments that do not have a local network configuration for discovery, we offer an enhanced AP onboarding experience that provides indication of the specific IP address or Fully-Qualified Domain Name (FQDN) of the controllers to which the AP connects.

With Enhanced Discovery, the user assigns a selection of APs to be managed by a specific controller (or high availability pair) as part of the conversion to local operating system. Once the AP boots into the local WiNG operating system, if the discovery override is defined, the AP automatically connects to the indicated controller, bypassing the traditional discovery methods.

Universal APs are configured for cloud management by default. To manage these APs locally, select **Local Management** when onboarding the APs in ExtremeCloud IQ.

In a remote deployment, you can configure the IP addresses or FQDNs of the primary and secondary controllers for local management. First, the AP uses a REST API call to connect to ExtremeCloud IQ. The API response includes the configured controller IP addresses. After the AP successfully adopts to ExtremeCloud IQ Controller, the access point reboots to the local management persona.

Enhanced Discovery is supported when manually onboarding devices or when importing devices with a .csv file.

Note
Enhanced Discovery is supported on AP3000. It requires ExtremeCloud IQ version 23.6.1 or greater.

Related Topics

Onboarding Universal APs — ExtremeCloud IQ on page 208
Local Onboarding — Manual Entry on page 212
Local Onboarding— Import CSV file on page 213

Local Onboarding — Manual Entry

From the **Setting Up Your Local Network** dialog, you can enter device serial numbers manually:

1. Select **Enter Manually**. Then, enter up to 10 device serial numbers separated by commas. The devices must all be the same model number.
2. Select the **Device OS**. For example, **WiNG**.
3. Optionally, select **Enhanced Discovery**.

   Select this option to define up to two specific controller IP addresses that the selected APs will register with for local service. Provide the IP address for the controllers. You have the option of defining a primary and secondary controller.

   Note
   Enhanced Discovery is supported on AP3000. It requires ExtremeCloud IQ version 23.6.1 or greater.

4. Select **Onboard Devices**.
5. Select **Finish**.

The APs display on the ExtremeCloud IQ Device List with the status **Onboarded**. New APs display the generic *HOSTNAME* because they are not yet registered with ExtremeCloud IQ. The AP Hostname automatically updates after the AP is powered on and connected into ExtremeCloud IQ.

Related Topics

Onboarding Universal APs — ExtremeCloud IQ on page 208
Local Onboarding— Import CSV file on page 213
Enhanced Discovery on page 211

Local Onboarding— Import CSV file

From the **Setting Up Your Local Network** dialog, you can import devices using a csv file:

1. If you have not already done so, create the CSV file. See below for an example of a CSV file.
2. Select **Import from CSV**.
3. Select **Choose** to navigate to the CSV file. Or, drag the file onto the dialog.
4. Select **Onboard Devices**.
5. Select **Finish**.

Enhanced Discovery — To take advantage of Enhanced Discovery while importing devices through CSV, formulate a multiple-column CSV file. For example:

Table 24: Example CSV file for Enhanced Discovery support

Serial Number	Primary Controller IP Address	Secondary Controller IP Address	Host Name
xxxxxxxxx-10004	10.xx.xxx.4	10.xx.xxx.5	
xxxxxxxxx-28887	10.xx.xxx.9	10.xx.xxx.6	

Note
Host Name will be supported in a future release of ExtremeCloud IQ.

Related Topics

Onboarding Universal APs — ExtremeCloud IQ on page 208
Local Onboarding — Manual Entry on page 212
Enhanced Discovery on page 211

Onboard a Controller to ExtremeCloud IQ

Onboard ExtremeCloud IQ Controller to your ExtremeCloud IQ account for Cloud Visibility into your network. Both a Navigator and a Pilot ExtremeCloud IQ account are supported.

Now, in addition to Universal APs that operate in either the cloud or on-premise, ExtremeCloud IQ Controller can operate in the cloud. All access points that are discovered by the controller are visible in ExtremeCloud IQ. This is not limited to Universal APs. The process of onboarding ExtremeCloud IQ Controller is similar to onboarding an access point.

Note
In a High Availability Pair, onboard the primary controller only to ExtremeCloud IQ for Cloud Visibility.

Before onboarding ExtremeCloud IQ Controller to ExtremeCloud IQ, install, configure, and license the controller. For more information, see configuration information under

Configuring DHCP, NPS, and DNS Services on page 25 and installation and licensing information under *ExtremeCloud IQ Controller documentation*.

The easiest way to onboard ExtremeCloud IQ Controller into ExtremeCloud IQ is to use the ExtremeCloud IQ Quick Add function.

Adding a Controller — Welcome Dialog

To onboard ExtremeCloud IQ Controller to ExtremeCloud IQ using the Welcome dialog, take the following steps:

1. Log into your ExtremeCloud IQ account and select

   Note
   The ExtremeCloud IQ Navigator or Pilot account is supported.

   The **Welcome** dialog displays.

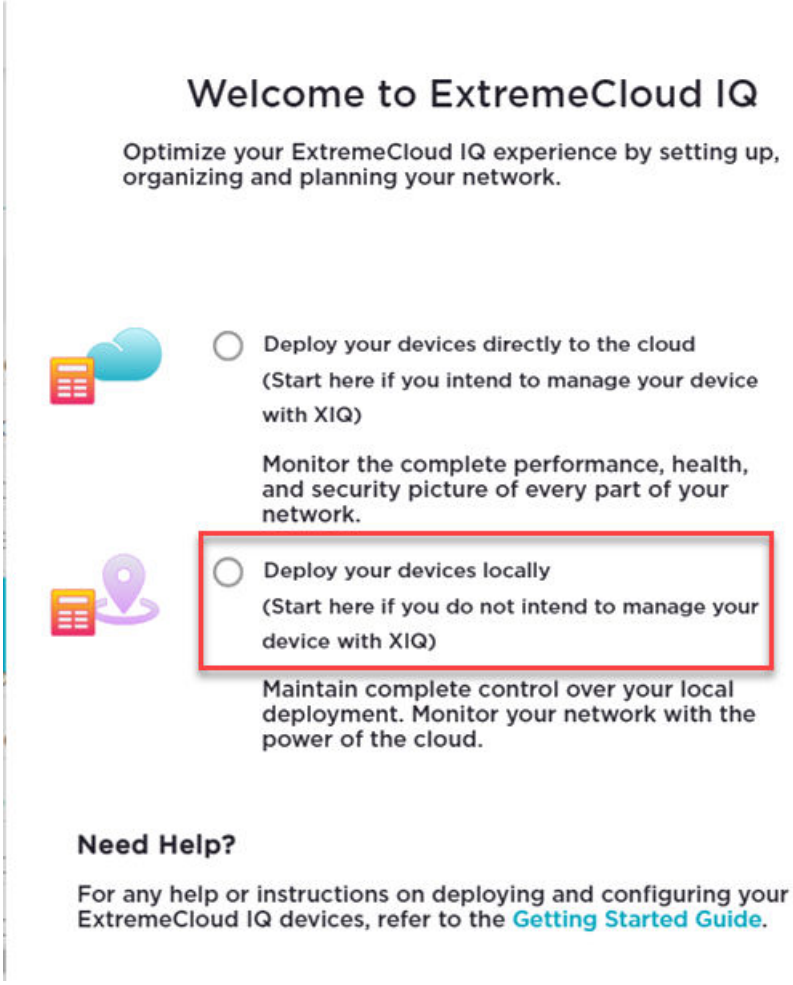
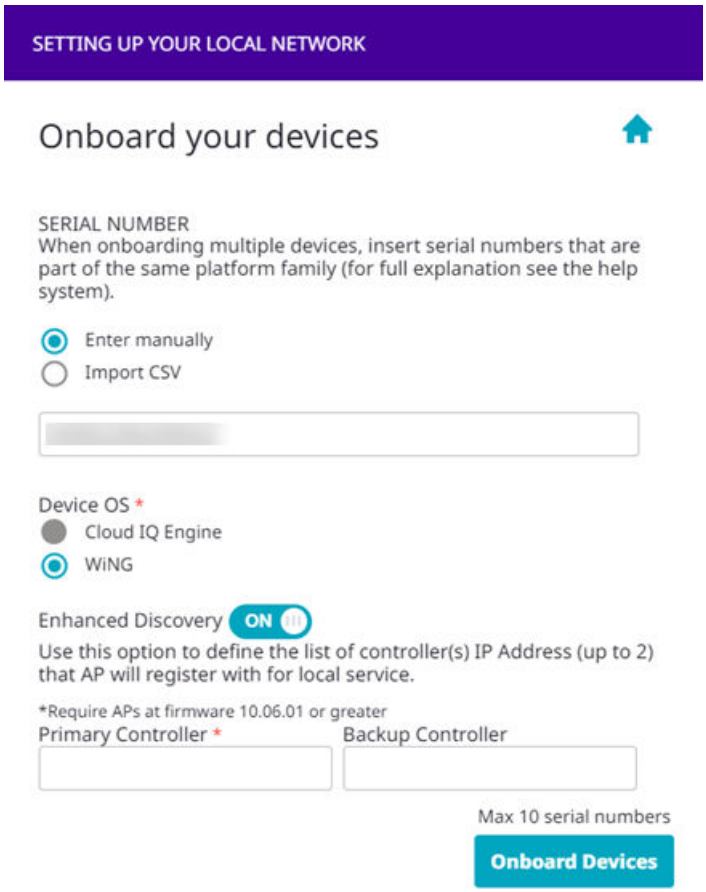


Figure 87: ExtremeCloud IQ Welcome Dialog

2. For ExtremeCloud IQ Controller, select **Deploy your devices directly to the cloud**.

3. On the next screen, select **Let's Get Started**.
4. Enter the ExtremeCloud IQ Controller serial number. This is the Locking ID of the controller. From the controller, go to **Administration** > **License** > **License Details**.
   - Type in serial numbers of the controller, separated by commas. Or,
   - Import from a CSV file.
     a. From the Device Make field, select **Controller**.
     b. Select **Choose** to navigate to the CSV file. Or, drag the file onto the dialog.



5. Select **Onboard Devices**.
6. Select **Finish**.

The controllers display on the ExtremeCloud IQ Device List with the status **Onboarded**. New controllers display the generic *HOSTNAME* because they are not yet registered with ExtremeCloud IQ. The controller hostname automatically updates after the AP is powered on and connected into ExtremeCloud IQ.

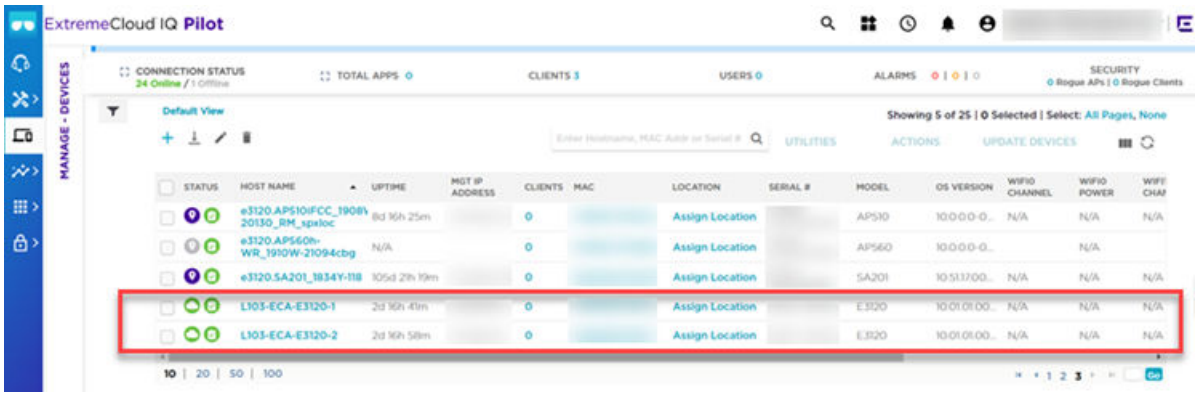


Figure 88: Controllers in Managed Devices List - ExtremeCloud IQ

Enhanced Discovery is supported on AP3000. It requires ExtremeCloud IQ version 23.6.1 or greater. The following is an optional way to change the primary and backup controllers.

1. Select the controller from the Managed Devices list.
2. Select **Actions** > **Enhanced Discovery**
3. Enter the **Primary Controller** IP address or FQDN, and the **Backup Controller** IP address or FQDN.
4. Select **OK**.

Add a Controller — Quick Add

To onboard ExtremeCloud IQ Controller to ExtremeCloud IQ using the Quick Add function, take the following steps:

1. From the ExtremeCloud IQ main navigation pane, select **Manage Devices**.
2. Select **Quick Add** (+).
3. In the Serial Number field, enter the ExtremeCloud IQ Controller serial number.

   This is the Locking ID of the controller. Find the controller Serial Number under the controller's License Details. From the controller, go to **Administration** > **License** > **License Details**.

   The **Device Make** field displays.

4. From the Device Make field, select **Controllers**.

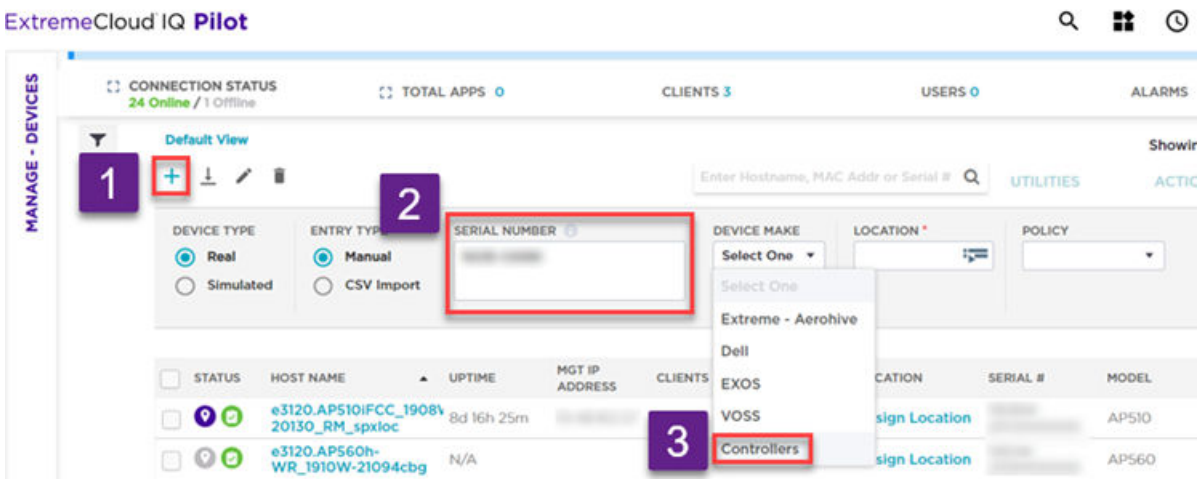


Figure 89: Manually adding a controller to ExtremeCloud IQ

The MAC Address field displays.

5. In the MAC Address field, enter the ExtremeCloud IQ Controller MAC Address.

   Find the controller MAC Address under the controller's License Details. From the controller, go to **Administration** > **License** > **License Details**.

6. Select **Add Devices**.

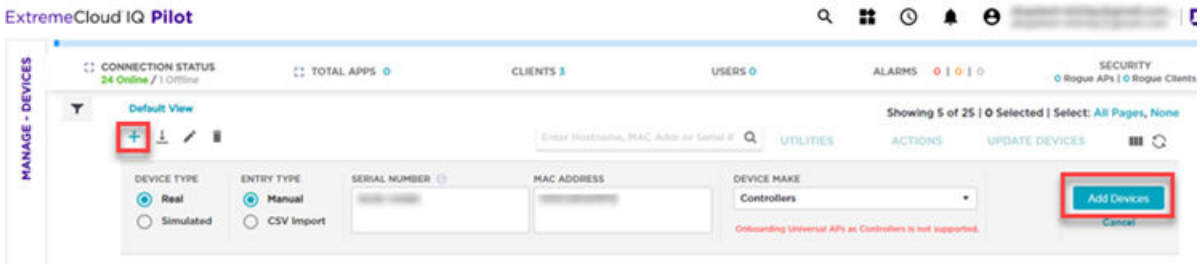


Figure 90: Controller Add Device Fields

The controller is added the list of managed devices.

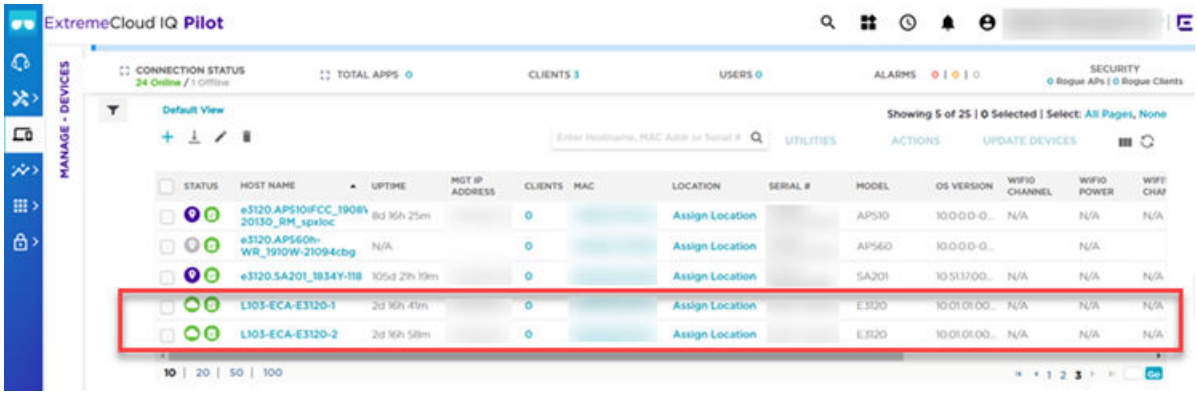


Figure 91: Controllers in Managed Devices List - ExtremeCloud IQ

Related Topics

Onboarding Universal APs — ExtremeCloud IQ on page 208

Access the Controller UI from ExtremeCloud IQ

To manage your devices from one pane of glass, access the ExtremeCloud IQ Controller user interface from ExtremeCloud IQ.

From your ExtremeCloud IQ Pilot account:

1. Go to **Manage**.

   The ExtremeCloud IQ **Device List** displays.
2. Select the Host Name for the ExtremeCloud IQ Controller.

   Details for the controller display.
3. From the left pane, scroll downward, then select **Configure** > **Appliance UI**.

   The user interface of the controller instance opens. You are automatically logged into ExtremeCloud IQ Controller with your ExtremeCloud IQ credentials.
4. Manage your devices.

Note

- All cloud user levels can log into ExtremeCloud IQ Controller from ExtremeCloud IQ, but you must have ExtremeCloud IQ Admin credentials to edit the controller configuration. All other ExtremeCloud IQ user types have read-only privileges on the controller.
- You can access one ExtremeCloud IQ Controller instance from ExtremeCloud IQ at a time.
- For best results, clear the browser cache after ExtremeCloud IQ is upgraded or after ExtremeCloud IQ Controller is rebooted.

PHP External Captive Portal, Controller's Firewall Friendly API

net-auth.php on page 219
login.php on page 223
common_utilities.php on page 225
crypt_aws_s4.php on page 229
ffecp-config.php on page 234

This section contains five files that serve as an example of how to build an External Captive Portal that makes use of the controller's Firewall-Friendly External Captive Portal Interface. The files presented are:

- net-auth.php

  Receives redirected requests from browsers trying to access web sites, verifies that the redirect was sent from the controller and if so, displays a suitable login page.
- login.php

  This script gets invoked as a consequence of a browser submitting the login form created by net-auth.php. The script authenticates the station in whatever way it likes. If the station is authorized, the script selects a maximum session duration and an access control role for the station. It then redirects the station's browser back to a web server on the controller, using a URI that contains the access control role, the maximum session duration, other data required by the controller, and a signature.
- crypt_aws_s4.php

  This file contains the code that verifies the signatures on received URLs and that signs the URLs that redirect the station back to the controller.
- common_utilities.php

  Utilities used by various ECP scripts.
- ffecp-config.php

  Contains the main statically configured parameters that the application uses to verify signed URLs and to create signed URLs.

net-auth.php

```
<?php
  // net-auth.php
```

```
// This is a simple implementation of a script that
// receives HTTP requests that have been redirected
// by a controller configured with "Firewall-Friendly
// External Captive Portal" support enabled.
// This script is responsible for collecting critical
// information from the redirection, such as the
// session token, and for constructing the login page
// for the user. The script reads the VNS attribute
// from the redirected request so that the script can
// display it on the login page.
//
// The script expects the controller to sign the
// redirection response. The script validates the
// signature. If the signature is valid, it displays
// the login page. Otherwise, it displays an error page.
//
// Assumptions
// ===========
// 1. The controller is configured to include its IP address
//    and port in the redirection URL.
// 2. The controller is configured to sign its redirection
//    responses using the Amazon S3 version 4 signature
//    algorithm (as of May 2014).
// 3. The controller is configured to include the VNS in its
// redirection response.
// 4. This application assumes that the Identity & Shared Key
// key pairs that it is allowed to use are stored in an associative
// array. It also assumes that some configuration options such
// as the 'service' and 'region' are stored in another associative
// array. Real applications might retrieve this information from
// a database or configuration file.

require_once("ffecp_config.php");
require_once("crypt_aws_s4.php");
require_once("common_utilities.php");

// Mainline processing starts here. Utilities are defined after
// the mainline.
// 1. Verify that the request has all necessary fields
// and a valid signature.
$rc = SimpleAws::verifyAwsUrlSignature(getURL($_SERVER),
 $awsKeyPairs);
if (SimpleAws::AWS4_ERROR_NONE != $rc) {
    printError(SimpleAws::getAwsError($rc));
    exit;
}
// Determines which controller interface to interact with
if(isset($_REQUEST['hwc_ip']) && isset($_REQUEST['hwc_port'])) {
  //BM IP address and port is enabled
  $hwc_ip = trim($_REQUEST['hwc_ip']);
  $hwc_port = trim($_REQUEST['hwc_port']);
} else {
  // The controller has not been configured as expected. It did not
  // include its address and port on the redirection URL. This is
  // easy to fix but all this program can do is report the error.
  printError("Controller must be configured to include its IP " .
  "address & port in the request.");
  exit;
}
// Collect the data required by the login page and
// subsequent authentication.
$dest = isset($_REQUEST['dest']) ? $_REQUEST['dest'] : "";
$bssid = isset($_REQUEST['bssid']) ? $_REQUEST['bssid'] : "";
$wlan = isset($_REQUEST['wlan']) ? $_REQUEST['wlan'] : "";
```

```
  $vns = isset($_REQUEST['vns']) ? $_REQUEST['vns'] : "";
  $mu_mac = isset($_REQUEST['mac']) ? $_REQUEST['mac'] : "";
  $ap_name = isset($_REQUEST['ap']) ? $_REQUEST['ap'] : "";
  $token = isset($_REQUEST['token']) ? $_REQUEST['token'] : "";
  if(!tokenCheck($token)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
token.</span>");
      exit;
  } else if(isset($hwc_port) && !is_numeric($hwc_port)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
port.</span>");
      exit;
  }else if($mu_mac && !macCheck($mu_mac)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
client MAC address.</span>");
      exit;
  } else if(!empty($wlan) && !is_numeric($wlan)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
WLAN.</span>");
      exit;
  }
   //escape the parameters
  $dest =convertUrlParam($dest);
  $bssid = convertUrlParam($bssid);
  $vns = convertUrlParam($vns);
  $ap_name = convertUrlParam($ap_name);
  // 3. Compose the login page and send it to the user. The page
  // is used to store session data. This could have been
  // stored in the user session variable or in cookies.
  print compose_login_page($hwc_ip, $hwc_port, $token, $dest,
           $wlan, $vns, $bssid, $mu_mac, $ap_name);
    // 4. And exit. This script is finished executing.
  exit;
  // End of mainline
  // A function that reconstructs the URL that the
  // station was trying to Get, from the variables
  // generated by the PHP runtime.
  function getURL($data) {
    $ssl = (!empty($data['HTTPS']) && $data['HTTPS'] == 'on') ? true:false;
    $protocol = $ssl ? "https" : "http";
    $port = $data['SERVER_PORT'];
    $port = ((!$ssl && $port=='80') || ($ssl && $port=='443')) ? '' :
   ':'.$port;
    $host = isset($data['HTTP_HOST']) ? $data['HTTP_HOST'] :
   $data['SERVER_NAME'] . $port;
    return $protocol . '://' . $host . $data['REQUEST_URI'];
  }
  // This function generates a basic login page containing a form
  // that allows the user to submit credentials back to this
  // server. The page displays the name of the VNS (service) that the user
  // is associated to.
  // A real login page normally has more content. This routine
  // highlights the critical aspects of composing a login page so
  // that when the user submits credentials, all the information
  // that is necessary to manage the user's session is on the page.
  function compose_login_page($hwc_ip, $hwc_port, $token, $dest,
          $wlan, $vns, $bssid, $mu_mac, $ap_name)
   {
     $template = "<!DOCTYPE html>
 <html>
 <head>
   <meta charset=\"ISO-8859-1\">
   <title>Please Login</title>
 </head>
```

```
<body>
  <form id=\"Login\" name=\"Login\" method=\"post\" action=\"login.php\">
    <table border='0' width='800' height='310' cellpadding='0'
      cellspacing='0'>
      <tr>
        <td colspan=\"3\" height=\"100\"> </td>
      </tr>
      <tr>
        <td width='260' height='1' border='0'/>
        <td width='300' height='65'>
          Please login to use '$vns' network.</td>
        <td width='240' rowspan='5'> </td>
      </tr>
      <tr>
        <td align=\"right\"><b>User Name  </b>
        </td>
        <td height=\"28\">
          <input type=\"text\" autocomplete=\"off\"
            id=\"userid\" name=\"userid\"
tabindex=\"1\">
        </td>
      </tr>
      <tr>
        <td align=\"right\"><b>Password  </b>
        </td>
        <td height=\"28\"><input type=\"password\"
autocomplete=\"off\"
          id=\"passwd\" name=\"passwd\" tabindex=\"2\">
        </td>
      </tr>
      <tr>
        <td><br>
        </td>
        <td height=\"33\" valign=\"bottom\"><input
type=\"submit\"
          style=\"width: 100px\" value=\"Login\"
tabindex=\"3\">
        </td>
      </tr>
    </table>
    <input type=\"hidden\" name=\"hwc_ip\" id=\"hwc_ip\"
value=\"$hwc_ip\"/>
    <input type=\"hidden\" name=\"hwc_port\" id=\"hwc_port\"
value=\"$hwc_port\"/>
    <input type=\"hidden\" name=\"token\" id=\"token\"
value=\"$token\"/>
    <input type=\"hidden\" name=\"dest\" id=\"dest\"
value=\"http://$dest\" />
    <input type=\"hidden\" name=\"wlan\" id=\"wlan\"
value=\"$wlan\" />
    <input type=\"hidden\" name=\"mu_mac\" id=\"mu_mac\"
value=\"$mu_mac\" />
    <input type=\"hidden\" name=\"bssid\" id=\"bssid\"
value=\"$bssid\" />
    <input type=\"hidden\" name=\"ap\" id=\"ap\"
value=\"$ap_name\" />
  </form>
</body>
</html>";
    return $template;
  }
?>
```

login.php

```
<?php
  // login.php
  // This is a simple implementation of a script that
  // receives a user's credentials, authenticates the
  // credentials, selects an access control role for
  // the user, then redirects the user back to the
  // controller using a signed URL containing the selected
  // access control role.
  // This script assumes that the credentials are
  // submitted on the form created by the example script
  // net-auth.php.
  //
  //
  // Assumptions
  // ===========
  // 1. The controller is configured to include its IP address
  //    and port in the redirection URL and the submitted login
  //    form contains that IP address and port. This allows the
  //    ECP to interact with more than one controller.
  // 2. Whether the script uses HTTP or HTTPS in its redirection
  //    response depends on the value of use_https,
  //    which must be defined in php.ini.
  //    If the value of use_https is 1, then the script uses
  //    HTTPS. If the configuration variable has any other value
  //    or is not defined, then the script uses HTTP. In practice,
  //    an actual site is going to settle on using HTTP or HTTPS.
  //    The scripts can then assume that method is being used
  //    rather than looking up the method in php.ini.
  // The use_https is a user-
  // defined variable. It must be created in php.ini by the
  // web server administrator.
  require_once("ffecp_config.php");
  require_once("crypt_aws_s4.php");
  require_once("common_utilities.php");
  // Some local constants
  const EWC_HTTP_REQ = "http://";
  const EWC_HTTPS_REQ = "https://";
  const EWC_REDIRECT_TARGET = "/ext_approval.php?";
  // The mainline begins here. The utilities are defined after the
  // mainline.
  // 1. Collect the parameters submitted on the login form.
  //    Some of these attributes come from hidden fields.
  $hwc_ip = trim($_REQUEST['hwc_ip']);
  $hwc_port = trim($_REQUEST['hwc_port']);
  $dest = trim($_REQUEST['dest']);
  $token = trim($_REQUEST['token']);
  $username = (isset($_REQUEST['userid'])) ?
    trim($_REQUEST['userid']) : "";
  $passwd = (isset($_REQUEST['passwd'])) ?
    trim($_REQUEST['passwd']) : "";
  $wlan = isset($_REQUEST['wlan']) ?
    trim($_REQUEST['wlan']) : "";
  if(!tokenCheck($token)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
token.</span>");
      exit;
  } else if(isset($hwc_port) && !is_numeric($hwc_port)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
port.</span>");
      exit;
  } else if(!empty($wlan) && !is_numeric($wlan)) {
      printError("Error: <span style='color:red'>Failed to process the request: incorrect
```

```
WLAN.</span>");
      exit;
  }
  // For this example the maximum duration of any user's
  // session will be 36000 seconds. The session is terminated
  // no later than this time. After the session is terminated,
  // the user can access the network but will be unauthenticated
  // again.
  $max_duration = 36000;
  // 2. Authenticate the user and select an appropriate role.
  //    Selecting the role is optional. If a role is not specified
  //    for the controller, the controller will apply the default
  //    authenticated role of the WLAN Service that the user is
  //    accessing.
  $assigned_role = authenticate($username, $passwd);
  if (false === $assigned_role) {
      // Failed to authenticate the user.
      // Authenticate prints the error message for
      // the browser and exits.
      exit;
  }
  // 3. Tell the controller that the user is authenticated,
  //    and tell it which role to apply to the user.
  //    3.a Build the URL that needs to be signed.
  $pUrl = makeUnsignedUrl($hwc_ip, $hwc_port, isHttps(), $token,
          $username, $wlan, $assigned_role, $dest,
          $max_duration);
  // 3.b Sign the URL. Otherwise, the role and session
  //     duration options will be ignored by the controller.
  $redirection = SimpleAws::createPresignedUrl(
    $pUrl, 'BigAuthInc', $awsKeyPairs['BigAuthInc'],
      $awsConfig['region'], $awsConfig['service'],
      $awsConfig['expires']);
  if (null == $redirection) {
      // Quietly exit. createPresignedUrl has already
      // reported an error to the browser.
    exit;
  }
  header( 'Location: '.$redirection);
  exit;
  // End of mainline.
  // A method that validates the user's credentials and
  // returns the role to apply to the user. In some cases,
  // this routine might also return the maximum session
  // duration in seconds.
  //
  // For purposes of this example, this procedure is
  // not much more than a stub. The stub can be replaced
  // by any authentication method, such as sending access
  // requests to a backend RADIUS server, or performing
  // a lookup in an application credential database.
  function authenticate($userid, $passwd) {
      if (("" == $userid) || ("" == $passwd)) {
          printError("Invalid Userid or Password. ".
                  "Please press the 'Back' button and try again.");
          // If you generate another login page for the user,
          // be sure to copy the hwc_ip address, hwc_port,
          // token and dest attributes from the submitted
          // login form to the login page.
          return false;
      } else {
          // Return the name of a role to be applied
          // to the station. The role must be defined on
          // the controller or it will substitute the
```

```
        // default authenticated role of the VNS that the
        // user is logging into.
        // For purposes of this example, assume all
        // authenticated users get the 'Guest_Access' role.
        return "Guest_Access";
    }
}
/**
 * A function that decides whether
 * to use HTTP or HTTPS in the redirect to
 * the controller. This example just uses
 * a php.ini user configuration variable
 * to decide.
 */
function isHttps() {
    if (get_cfg_var('use_https')) {
        if (1 == get_cfg_var('use_https')) {
            $useHttps = true;
        } else {
            $useHttps = false;
        }
    } else {
        $useHttps = false;
    }
    return $useHttps;
}
/**
 * A method that assembles an unsigned URL out of the
 * the input from the user's succesful login
 * @param string  $hwc_ip     IP or FQDN of controller
 * @param int     $hwc_port   Port on controller to receive redirection
 * @param bool    $useHttps   Whether the redirect uses HTTP or HTTPS
 * @param string  $token      Identifier for the station's session
 * @param string  $username   The name the station's user logged in with
 * @param int     $wlanid     Identifier for the WLAN the station is using
 * @param string  $assigned_role Name of the access control role to assign
 * @param string  $dest       The URL the station was trying to get to
 * @param int     $max_duration The maximum length of the station's session.
 */
function makeUnsignedUrl($hwc_ip, $hwc_port, $useHttps, $token,
        $username, $wlanid, $assigned_role, $dest,
        $max_duration) {
     $redirectUrl = ($useHttps ? EWC_HTTPS_REQ : EWC_HTTP_REQ)
        .$hwc_ip;
     if ((80 != $hwc_port) && (443 != $hwc_port)) {
         $redirectUrl .= ":".$hwc_port;
     }
     $redirectUrl .= EWC_REDIRECT_TARGET
        .'token='. rawurlencode($token)
        .'&wlan='.rawurlencode($wlanid)
        .'&username='.rawurlencode($username)
        .(is_not_empty($dest) ?'&dest='.rawurlencode($dest):'')
        .(is_not_empty($assigned_role) ? '&role='.
                rawurlencode($assigned_role):'')
        .(is_not_empty($max_duration) ?'&opt27='.$max_duration:'');
     return $redirectUrl;
}
?>
```

common_utilities.php

```
<?php
  // A library of utilities that can be used by PHP scripts
```

```
  // comprising an external captive portal.
  // A utility that translates error codes to error messages.
  function code_2_message($code, $content_type)
  {
    $errMsgList = array (
      0 =>
      array (
        'label' => 'Invalid',
        'content' => '<span style=\'color:red\'>Empty id /
password not allowed. Please try again.</span>'
      ),
      1 =>
      array (
        'label' => 'Success',
        'content' => 'Success',
      ),
      2 =>
      array (
        'label' => 'Access Fail',
        'content' => '<span style=\'color:red\'>Userid or
password incorrect. Please try again.</span>',
      ),
      3 =>
      array (
        'label' => 'Fail',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      4 =>
      array (
        'label' => 'Timeout',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      5 =>
      array (
        'label' => 'RADIUS shared security key fail',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      6 =>
      array (
        'label' => 'RADIUS internal error',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      7 =>
      array (
        'label' => 'Max RADIUS login fail',
        'content' => '<span style=\'color:red\'>Too many users
trying to login at the same time.Please try again later.</span>',
      ),
      8 =>
      array (
        'label' => 'Invalid Login parameters',
        'content' => '<span style=\'color:red\'>Userid or
password incorrect. Please try again.</span>',
      ),
      9 =>
      array (
```

```
        'label' => 'General failure',
        'content' => '<span style=\'color:red\'>A problem has
occurred while trying to validate your userid & password.<br>Please contact
your system administrator.</span>',
      ),
      14 =>
      array (
        'label' => 'Invalid third party parameters',
        'content' => '<span style=\'color:red\'>Invalid third
party parameters.</span>',
      ),
      15 =>
      array (
        'label' => 'Authentication in progress failure',
        'content' => '<span style=\'color:red\'>Authentication is
in progress.</span>',
      ),
      17 =>
      array (
        'label' => 'Max concurrent session failure',
        'content' => '<span style=\'color:red\'>Login rejected
because the maximum number of concurrent sessions for this set of credentials
has been reached. Please try again later.</span>',
      ),
      18 =>
      array (
        'label' => 'Identified session not found',
        'content' => '<span style=\'color:red\'>Login failed
because could not find a session for the specified identifiers.</span>'
      ),
      99 =>
      array (
        'label' => 'Timeout while trying to authorize a session',
        'content' => '<span style=\'color:red\'>Login failed
because because the controller took too long to authorize the
session.</span>'
      )
      );
      return (isset($errMsgList[$code])) ?
        $errMsgList[$code][$content_type] :
        "Unrecognized error code: ".$code;
  }
  // General purpose error reporting procedure.
  function printError($errorMsg) {
    header('Content-type: text/html; charset=iso-8859-1');
    print
"<html>\n<head><title>Error</title></head><body>\n<p>\n$errorMsg\n</p>\n</bod
y>\n</html>\n";
  }
  // Use base64 url safe encode/decode when dealing
  // with AES-encrypted strings.
  // encode: '+'=>'-', '/' => '_' , '=' => '!'
  function base64_url_encode($input) {
    return strtr(base64_encode($input), '+/=', '-_!');
  }
  // Decode: '-'=>'+', '_' => '/' , '!' => '='
  function base64_url_decode($input) {
    return base64_decode(strtr($input, '-_!', '+/='));
  }
  // xml parsing functions
  function my_xml2array($contents)
  {
    $xml_values = array();
    if (! isset($contents)) {
```

```
      return false;
    }
    $parser = xml_parser_create('');
    if(!$parser) {
      return false;
    }
    xml_parser_set_option($parser, XML_OPTION_TARGET_ENCODING,
                  'UTF-8');
    xml_parser_set_option($parser, XML_OPTION_CASE_FOLDING, 0);
    xml_parser_set_option($parser, XML_OPTION_SKIP_WHITE, 1);
    xml_parse_into_struct($parser, trim($contents), $xml_values);
    xml_parser_free($parser);
    if (!$xml_values) {
      return array();
    }
    $xml_array = array();
    $last_tag_ar =& $xml_array;
    $parents = array();
    $last_counter_in_tag = array(1=>0);
    foreach ($xml_values as $data)
    {
      switch($data['type'])
      {
        case 'open':
          $last_counter_in_tag[$data['level']+1] = 0;
          $new_tag = array('name' => $data['tag']);
          if(isset($data['attributes']))
          $new_tag['attributes'] = $data['attributes'];
          if(isset($data['value']) && trim($data['value']))
          $new_tag['value'] = trim($data['value']);
          $last_tag_ar[$last_counter_in_tag[
$data['level']]] = $new_tag;
          $parents[$data['level']] =& $last_tag_ar;
          $last_tag_ar =& $last_tag_ar[
            $last_counter_in_tag[$data['level']]++];
          break;
        case 'complete':
          $new_tag = array('name' => $data['tag']);
          if(isset($data['attributes']))
          $new_tag['attributes'] = $data['attributes'];
          if(isset($data['value']) &&
            trim($data['value']))
          $new_tag['value'] = trim($data['value']);
          $last_count = count($last_tag_ar)-1;
            $last_tag_ar[ $last_counter_in_tag[$data[
'level' ]]++ ] = $new_tag;
          break;
        case 'close':
          $last_tag_ar =& $parents[$data['level']];
          break;
        default:
          break;
      };
    }
    return $xml_array;
  }
  function get_value_by_path($__xml_tree, $__tag_path)
  {
    $tmp_arr =& $__xml_tree;
    $tag_path = explode('/', $__tag_path);
    foreach($tag_path as $tag_name)
    {
      $res = false;
      foreach($tmp_arr as $key => $node)
```

```
      {
        if(is_int($key) && $node['name'] == $tag_name)
        {
          $tmp_arr = $node;
          $res = true;
          break;
        }
      }
      if(!$res) {
        return false;
      }
    }
    if( isset($tmp_arr['value']) ) {
      return $tmp_arr['value'];
    } else {
      return null;
    }
  }
  function is_not_empty($string) {
    return (isset($string) && (0 < strlen($string)));
  }
  //check token format
    function tokenCheck($val){
        return preg_match('/^([a-zA-Z0-9-_!]){0,24}$/', $val);
    }
    //check the mac address
    function macCheck($val){
        return preg_match("/^[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}:
[A-Fa-f0-9]{2}:[A-Fa-f0-9]{2}$/", $val);
    }
    //encode the input string to avoid script attack
    function convertUrlParam($input) {
        return htmlentities($input, ENT_QUOTES);
  }
?>
```

crypt_aws_s4.php

Note

The External Captive Portal and ExtremeCloud IQ Controller must be time synchronized. AWS4 signature includes a time stamp; therefore, both systems must be configured with the correct date and time when using AWS4 signature.

```
<?php
class SimpleAws {
    const     AWS4_ERROR_NONE=0;
    const     AWS4_ERROR_NULL_INPUT=1;
    const     AWS4_ERROR_INPUT_BUFFER_TOO_SMALL=2;
    const     AWS4_ERROR_INVALID_PROTOCOL=3;
    const     AWS4_ERROR_INPUT_URL_TOO_BIG=4;
    const     AWS4_ERROR_INPUT_ID_TOO_BIG=5;
    const     AWS4_ERROR_INPUT_KEY_TOO_BIG=6;
    const     AWS4_ERROR_INVALID_REGION=7;
    const     AWS4_ERROR_INVALID_SIGNATURE=8;
    const     AWS4_ERROR_MISSING_QUERY=9;
    const     AWS4_ERROR_MISSING_QUERY_DATE=10;
    const    AWS4_ERROR_MISSING_QUERY_SIGNED_HEADERS=11;
    const    AWS4_ERROR_MISSING_QUERY_EXPIRES=12;
    const    AWS4_ERROR_MISSING_QUERY_SIGNATURE=13;
    const    AWS4_ERROR_MISSING_QUERY_CREDENTIAL=14;
```

```
    const    AWS4_ERROR_MISSING_QUERY_ALGORITHM=15;
    const    AWS4_ERROR_MISSING_QUERY_PARAMS=16;
    const    AWS4_ERROR_MISSING_CRED_PARAMS=17;
   const     AWS4_ERROR_STALE_REQUEST=2001;
   const     AWS4_ERROR_UNKNOWN_IDENTITY=2002;
    const     AWS4_EXTREME_REQUEST="aws4_request";
    const     AWS4_MAX_URL_SIZE= 512;
    const     AWS4_HTTP_REQ = "http://";
    const     AWS4_HTTPS_REQ= "https://";
    const     AWS4_MANDATORY_CRED_PARAMS = 4;
    /**
     * Method to verify the AWS signature based on given full URL address.
         *
     * @param string $pUrl
     * @param array $awsKeyPairs identity, shared secret key pairs
     * @return AWS error code
     */
    public static function verifyAwsUrlSignature($pUrl,
        $awsKeyPairs) {
          // Perform basic validation
        if($pUrl==NULL) {
            return self::AWS4_ERROR_NULL_INPUT;
        }
        if (2*self::AWS4_MAX_URL_SIZE < strlen($pUrl)) {
            return self::AWS4_ERROR_INPUT_URL_TOO_BIG;
        }
        if(stripos($pUrl, self::AWS4_HTTP_REQ)!=0 || stripos($pUrl, self::AWS4_HTTPS_REQ)!
=0) {
            return self::AWS4_ERROR_INVALID_PROTOCOL;
        }
        $urlParams = parse_url($pUrl);
        if (!isset($urlParams['query'])) {
            return self::AWS4_ERROR_MISSING_QUERY;
        }
        $queryParams = explode("&", $urlParams['query']);
        foreach($queryParams AS $el) {
            $arr = explode("=", $el);
            $q[$arr[0]] = $arr[1];
        }
        $valResult = self::validateQueryParms($q);
        if (self::AWS4_ERROR_NONE != $valResult) {
            return $valResult;
        }
        // Done with the basic validations.
        $date = $q['X-Amz-Date'];
        $sign = $q['X-Amz-Signature'];
        $credentVal = rawurldecode($q['X-Amz-Credential']);
        ksort($q);
        // Remove the signature from the list of parameters over
        // which the signature will be recomputed.
        unset($q['X-Amz-Signature']);
        $credentAttrs = explode("/", $credentVal);
        $pKey = $credentAttrs[0];
        if (self::AWS4_MAX_URL_SIZE < strlen($pKey)) {
            return self::AWS4_ERROR_INPUT_KEY_TOO_BIG;
        }
        if(self::AWS4_MANDATORY_CRED_PARAMS > count($credentAttrs)) {
            return self::AWS4_ERROR_MISSING_CRED_PARAMS;
        }
       if (!isset($awsKeyPairs[$pKey])) {
            return self::AWS4_ERROR_UNKNOWN_IDENTITY;
       }
        $scope = $credentAttrs[1]."/".$credentAttrs[2]."/"
         .$credentAttrs[3]."/".$credentAttrs[4];
```

```
      $port = $urlParams['port'];
       $host = strtolower($urlParams['host']);
        if($port && (($urlParams['scheme']=='https' && $port !=
         443)||($urlParams['scheme']=='http' && $port != 80))) {
            $host .= ':'.$port;
        }
        $canonical_request = self::getCanonicalFFECPContent($q,
            $host, $urlParams['path']);
        $stringToSign = "AWS4-HMAC-SHA256\n{$date}\n{$scope}\n" .
          hash('sha256', $canonical_request);
        $signingKey = self::getSigningKey($credentAttrs[1], $credentAttrs[2],
            $credentAttrs[3], $awsKeyPairs[$pKey]);
        $mySign = hash_hmac('sha256', $stringToSign, $signingKey);
        if (strcmp($mySign,$sign)){
            return self::AWS4_ERROR_INVALID_SIGNATURE;
        }
        return self::AWS4_ERROR_NONE;
    }
    /**
     * Method to verify that the query parameters contain the elements
     * required in the response to the controller and the ones required to
     * sign the request.
     * @param array $qParams: an associative array in which the key of an
     * entry is the name of a query parameter and the corresponding value
     * is the value of that parameter.
     * @return an AWS_ERROR code.
     */
     private static function validateQueryParms($qParams) {
         if (is_null($qParams)) {
             return self::AWS4_ERROR_MISSING_QUERY;
         }
         if ((!isset($qParams['wlan'])) or (!isset($qParams['token']))
            or (!isset($qParams['dest']))) {
            return self::AWS4_ERROR_MISSING_QUERY_PARAMS;
         }
         if (!isset($qParams['X-Amz-Signature'])) {
             return self::AWS4_ERROR_MISSING_QUERY_SIGNATURE;
         }
         if(!isset($qParams['X-Amz-Algorithm'])) {
             return self::AWS4_ERROR_MISSING_QUERY_ALGORITHM;
         }
         if (!isset($qParams['X-Amz-Credential'])) {
             return self::AWS4_ERROR_MISSING_QUERY_CREDENTIAL;
         }
         if (!isset($qParams['X-Amz-Date'])) {
             return self::AWS4_ERROR_MISSING_QUERY_DATE;
         }
         if (!isset($qParams['X-Amz-Expires'])) {
             return self::AWS4_ERROR_MISSING_QUERY_EXPIRES;
         }
         if (!isset($qParams['X-Amz-SignedHeaders'])) {
             return self::AWS4_ERROR_MISSING_QUERY_SIGNED_HEADERS;
         }
         // The date & expires parameters exist in the request.
         // Verify that the request is not stale or replayed.
         $redirectedAt = DateTime::createFromFormat('Ymd?Gis?',
            $qParams['X-Amz-Date'], new DateTimeZone("UTC"));
         $expires = $qParams['X-Amz-Expires'];
         $now = date_create();
         $delta = $now->getTimestamp() - $redirectedAt->getTimestamp();
         // The following gives some latitude for clocks that are not synched
         if (($delta < -10) or ($delta > $expires)) {
             print("<br>");
             print(date("Y-m-d H:i:sZ", $now->getTimestamp()));
```

```
            print("<br>");
               print("Redirected at: ");
            print(date("Y-m-d H:i:sZ", $redirectedAt->getTimestamp()));
            print("<br>");
               print($now->getTimeZone()->getName());
            print("<br>");
        print($redirectedAt->getTimeZone()->getName());
               print("<br>");
            print($expires);
            print("<br>");
            print($delta);
           return self::AWS4_ERROR_STALE_REQUEST;
         }
         return self::AWS4_ERROR_NONE;
     }
    /**
     * Method to generate the AWS signed URL address
     * @param string $pUrl: the URL that need to be appended with AWS parameters
     * @param string $identity: the AWS identity
     * @param string $sharedSecret: the secret shared with the controller
     * @param string $region:  the region component of the scope
     * @param string $service: the service component of the scope
     * @param int $expires: number of seconds till presigned URL is untrusted.
     * @return URL string with AWS parameters
     */
    public static function createPresignedUrl(
        $pUrl, $identity, $sharedSecret, $region,
        $service, $expires) {
        $urlParams = parse_url($pUrl);
        $httpDate = gmdate('Ymd\THis\Z', time());
        $scopeDate = substr($httpDate, 0, 8);
        $scope = "{$scopeDate}/".$region."/".$service."/".self::AWS4_EXTREME_REQUEST;
        $credential = $identity . '/' . $scope;
        $duration = $expires;
        //set the aws parameters
        $awsParams = array(
            'X-Amz-Date'=>$httpDate,
            'X-Amz-Algorithm'=> 'AWS4-HMAC-SHA256',
            'X-Amz-Credential'=> $credential,
            'X-Amz-SignedHeaders' =>'host',
            'X-Amz-Expires'=> $duration
        );
        parse_str($urlParams['query'],$q);
        $q = array_merge($q, $awsParams);
        ksort($q);
      $port = $urlParams['port'];
       $host = strtolower($urlParams['host']);
        if($port && (($urlParams['scheme']=='https' && $port !=
         443)||($urlParams['scheme']=='http' && $port != 80))) {
            $host .= ':'.$port;
        }
        $canonical_request = self::getCanonicalFFECPContent($q,
         $host, $urlParams['path'], true);
        $stringToSign = "AWS4-HMAC-SHA256\n{$httpDate}\n{$scope}\n" .
            hash('sha256', $canonical_request);
        $signingKey = self::getSigningKey(
                $scopeDate,
                $region,
                $service,
                $sharedSecret
        );
        $q['X-Amz-Signature'] = hash_hmac('sha256', $stringToSign,
                $signingKey);
        $p = substr($pUrl, 0, strpos($pUrl,'?'));
```

```
        $queryParams = array();
        foreach($q AS $k=>$v) {
            $queryParams[] = "$k=".rawurlencode($v);
        }
        $p .= '?'.implode('&', $queryParams);
        return $p;
    }
    /**
     * Method to generate the AWS signing key
     * @param string $shortDate: short date format (20140611)
     * @param string $region: Region name (us-east-1)
     * @param string $service: Service name (s3)
     * @param string $secretKey Secret Access Key
     * @return string
     */
    protected static function getSigningKey($shortDate, $region, $service, $secretKey) {
        $dateKey = hash_hmac('sha256', $shortDate, 'AWS4' . $secretKey, true);
        $regionKey = hash_hmac('sha256', $region, $dateKey, true);
        $serviceKey = hash_hmac('sha256', $service, $regionKey, true);
        return  hash_hmac('sha256', self::AWS4_EXTREME_REQUEST, $serviceKey, true);
    }
    /**
     * Create the canonical context for the AWS service
     * @param array $queryHash the query parameter hash
     * @param string $host host name or ip address for the target service
     * @param string $path the service address for the target service
     * @param boolean $encode determine if the query parameter need to be encoded or not.
     * @return string the canonical content for the request
     */
    protected static function getCanonicalFFECPContent($queryHash, $host, $path,
$encode=false) {
        $queryParams = array();
        foreach($queryHash AS $k=>$v) {
            if($encode) {$v = rawurlencode($v);}
        $queryParams[] = "$k=$v";
         }
         $canonical_request = "GET\n"
            .$path."\n"
            .implode('&',$queryParams)."\n"
            .'host:'.$host
            ."\n\nhost\nUNSIGNED-PAYLOAD";
         return $canonical_request;
    }
    /**
     * Create user readable error message
     * @param integer $eid error code after verifying the AWS URL
     * @return string the error message
     */
    public static function getAwsError($eid) {
        $forAws = " for Amazon Web Service request.";
        SWITCH ($eid) {
            case self::AWS4_ERROR_NULL_INPUT:
                $res = "Empty input".$forAws;
            break;
            case self::AWS4_ERROR_INPUT_BUFFER_TOO_SMALL:
                $res = "Input buffer is too small".$forAws;
            break;
            case self::AWS4_ERROR_INVALID_PROTOCOL:
                $res = "Invalid protocol".$forAws;
            break;
            case self::AWS4_ERROR_INPUT_URL_TOO_BIG:
                $res = "Input url is too big".$forAws;
            break;
            case self::AWS4_ERROR_INPUT_ID_TOO_BIG:
```

```
                $res = "Input ID is too big".$forAws;
            break;
            case self::AWS4_ERROR_INVALID_REGION:
                $res = "Invalid region".$forAws;
            break;
            case self::AWS4_ERROR_INVALID_SIGNATURE:
                $res = "Invalid signature".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY:
                $res = "Missing all query parameters".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_DATE:
                $res = "Missing query date".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_SIGNED_HEADERS:
                $res = "Missing query signed headers".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_EXPIRES:
                $res = "Missing query expires".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_SIGNATURE:
                $res = "Missing query signature".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_CREDENTIAL:
                $res = "Missing query credential".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_ALGORITHM:
                $res = "Missing query algorithm".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_QUERY_PARAMS:
                $res = "Missing query parameter".$forAws;
            break;
            case self::AWS4_ERROR_MISSING_CRED_PARAMS:
                $res = "Missing credential parameters".$forAws;
            break;
            case self::AWS4_ERROR_STALE_REQUEST:
                $res = "Invalid request date".$forAws;
            break;
            case self::AWS4_ERROR_UNKNOWN_IDENTITY:
                $res = "Unrecognized identity or identity without a shared secret.";
            break;
            default:
                $res = "Successfully validated".$forAws;
            break;
        }
        return $res;
    }
    /**
     * Return the AWS validation error message
     * @param string $pUrl
     * @return string the error message
     */
    public function getUrlValidationResult($pUrl) {
        $eid = self::verifyAwsUrlSignature($pUrl);
        return self::getAwsError($eid);
     }
  }
?>
```

ffecp-config.php

```
<?php
  // This file contains PHP associative arrays holding the relatively
```

```
  // static configuration for this ECP application. A real application
  // might read the data in from an XML or '.ini' file.
  // An associative array of identity => shared secret pairs.
  // This example only uses the first one. Any printable ASCII
  // alphanumeric string can be use for the identity and shared
  // secret so long as both the ECP and the controller use the
  // same pair.
  $awsKeyPairs = array(
      'BigAuthInc'=>'secretferqrer123456667',
      'testingidentity1'=>'secretferqrer123456668',
      'testingidentity2'=>'secretferqrer123456669'
  );
  // Aws Signature-related Configuration
  // Region and service are used to build the scope.
  // Expires is the maximum amount of time the signed URL
  // should be trusted.
  $awsConfig = array(
      'region' => 'world',
      'signature'=> 'v4',
      'service'=>'ecp',
      'expires'=>60
  );
?>
```

Index

A

AAA configuration
    network policy configuration 128, 145
    RADIUS settings 93, 135
AAA Network, Default Auth Role accept policy 86
AAA Network, Pass-thru External RADIUS Accept Policy 89
Access Control Group 120
Access Control Groups 121
Access Control Rule 123
Access Control Rules
    proprietary port 119
Access Control Rules, default 125
adoption rules,
    creating 65
AirDefense 199, 200
announcements x
AP Client Bridge 189
appliance specifications 14
availability pair 196, 199
Availability pair with AirDefense 199
availability pair, switches 22

B

B@AC network topology 60

C

Captive Portal, ExtremeGuest 185
captive portal, internal
    configuring 59
Centralized Web Authentication 128, 145
Centralized Web Authentication (CWA)
    authorization policy on Cisco server 141
    authorization policy on CWA server 141, 154
    authorization policy on ExtremeControl server 154
    CWA network settings 136, 149
Centralized Web Authentication (CWA) captive portal
    CWA Policy Redirection Role Settings 139, 152
Centralized Web Authorization
    AAA Policy settings 131
Cisco ISE 128
Client Bridge
    configure 191
cloud integration
    controller log in 218
conventions
    notice icons vii
conventions *(continued)*
    text vii

D

Default Auth Role 85
Default Pass-Through Rule 168
Defender for IoT 18, 19
Deploying Universal APs 207
device groups
    modifying 63, 71, 206
    overview 23
    profile settings 63, 206
DHCP
    add new scope 26
    configure server options 32
    create new options 30
    local management 53
    Option 078 30
    Option 43 34
    Vendor Class Identifier 34
    Windows Server 2012 R2 25
discovery and registration 17
discovery, APs and adapters, Centralized site 18, 19
discovery, Centralized site APs and adapters 19
discovery, switches 20, 21
documentation
    feedback ix
    location ix

E

EGuest, configuring network 186
engine rules,
    B@AC captive portal 62
    creating rules 69
External Captive Portal
    configuring network 203
External Captive Portal, configuring network 164
External Captive Portal, ExtremeCloud IQ - Site Engine 163
External NAC server to authenticate client sessions 82
Extreme Management Center (XMC)
    ExtremeCloud IQ - Site Engine 163
ExtremeCloud IQ - SE, unregistered policy 175
ExtremeCloud IQ - Site Engine 163
ExtremeCloud IQ - Site Engine profile for external captive portal 177
ExtremeControl 145

ExtremeGuest 185
ExtremeGuest configuration 187
ExtremeGuest server settings 186

F

feedback ix

L

Local DHCP Settings 55

M

MBA Network, Default Auth Role accept policy 85
MBA Network, Pass-thru External RADIUS accept policy 88
Mesh Point Network
    Transparent Bridge 80

N

NAC Server, configuring external server 83
NAI Routing
    AAA Policy settings 158
    regular expression realm 161
network topology, B@AC 60
networks
    AAA Network 68
    WPAv2 PSK 61
notices vii

O

onboarding
    advanced discovery 211
    controller 208, 211–213
    import csv 213
    remote deployments 211
    Universal APs 208, 211–213

P

Pass-Through External RADIUS accept policy 88
policy role, Admin Access 122, 126
policy role, creating 70
precedence 126
product announcements x
profile settings 63, 71, 200, 206
profile, edit 168
profile, external captive portal 177

R

RADIUS servers
    advanced settings 93
    for user authentication 92
    settings 93, 135
role, creating 70

S

sites
    overview 22
sites,
    adding a Centralized Site 57
support, *see* technical support
switch, Controller as a switch 170
switches discovery 20, 21
switches, availability pair 22

T

technical support
    contacting x

U

Universal APs
    onboarding 208, 211–213
unregistered policy 175
user authentication, RADIUS servers 92

W

warnings vii

X

XMC
    ExtremeCloud IQ - Site Engine 163